144

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07C 13/00 — A1

(11) International Publication Number: **WO 96/02044**

(43) International Publication Date: 25 January 1996 (25.01.96)

(21) International Application Number: PCT/US95/08267

(22) International Filing Date: 7 July 1995 (07.07.95)

(30) Priority Data:
08/272,068 8 July 1994 (08.07.94) US

(60) Parent Application or Grant
(63) Related by Continuation
US 08/272,068 (CON)
Filed on 8 July 1994 (08.07.94)

(71) Applicant *(for all designated States except US)*: VOTATION CORPORATION [US/US]; 18004 Calico Circle, Olney, MD 20832 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: WILLARD, Jim, P. [US/US]; 18004 Calico Circle, Olney, MD 20832 (US).

(74) Agent: MARLETTE, Todd, Edward; Suite 1210 North, 2111 Jefferson Davis Hwy., Arlington, VA 22202-3134 (US).

(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GB, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: REMOTE RECORDING COMPUTER VOTING SYSTEM

(57) Abstract

An electronic voting system provides cost effective, automated, secure, and tamper-proof public elections. The voting system provides election support from the precinct-level up to and including the state and national levels. The voting system is single-use, disposable and utilizes logical processing control functions and electronic ballots. An electronic security access key card enables voter access. Votes are collected and tabulated both directly and remotely using a hierarchical remote control. Local and remote monitoring provide testing, failure detection, repairs, and operational monitoring and control functions. On-line election certification, as well as off-line election certification are also provided. Audit trail recording and voter record recording allow for a checking mechanism and may be used for on-line statistical data collection and displays.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

Title of the Invention

REMOTE RECORDING COMPUTER VOTING SYSTEM

Field of the Invention:

This invention relates to automated and/or electronic voting systems used for conducting public elections. A single-use design is disclosed in which certain components are manufactured specifically for use in one election. A system is also disclosed that provides a voter interface allowing votes to be cast, recorded, and tabulated in a secure manner using logical functions to automate the process. Remote recording is also used to facilitate the rapid, centralized collection of votes. The above system performs the above-mentioned functions while maintaining voter anonymity.

Background of the Invention:

Many prior designs have attempted to utilize computer based equipment and programs to count votes during public elections. Prior art systems have generally attempted to computerize the functions of mechanical voting machines and have attempted to integrate the complete process of voting, such as registration. However, in some cases, the desire to "automate" and/or "integrate" various functions and to provide "adaptive" systems has resulted in undue complexity. Prior designs have also overemphasized reusability without the consideration of economic feasibility.

A number of prior art systems have provided automated voting systems. Wise et al., U.S. Patent No. 5,218,528, disclose a system which "integrates the stages of registering and certifying voters and collecting their votes". They further disclose the incorporation of an "interactive graphic interface for vote entry". This type of system takes advantage of existing technology and provides some desirable attributes. However, such a design adds greatly to the system's complexity and cost. In addition, the implementation described does not provide for operation in some states where a "full face ballot" must be used. (The term "full face ballot" describes a ballot

in which all candidates for all electoral races must be presented to the voter at once. At the present time, some states require this type of ballot.) Additionally, the Wise et al. design requires the voter to exercise control over the system operation by performing more actions than necessary to cast a vote. These include selecting a presentation language, paging through the election races on screen, and physically entering an access code. While these operational aspects may provide greater adaptivity, they are not desirable for quick and efficient voting.

Boram, U.S. Patent 4,641,240, discloses an electronic voting machine and system. While Boram allows for computer control of voting, important system concerns are not addressed. The design essentially replicated the function of the mechanical voting machines it was intended to replace. However, it also replicated the problems and limitations of the mechanical voting machine. Boram describes a process whereby the ballot is comprised of push-button switches arranged in rows and columns and overlaid with a printed list of candidates and issues. However, this presents a potential for breech of security either through accident or through planned tampering. The potential exists since the list could be intentionally moved or accidentally placed over switches which do not record the voters intended vote.

Boram also uses the limited row and column layout typical of older mechanical voting machines. This type of layout constrains the ballot design to fit within the rows and columns defined by the physical attributes of the machine. This type of layout does not possess the capability of being connected to a centralized processor for control and vote tallying. Life cycle costs of this design would be substantial due to the obsolescence of available parts, the transportation and storage costs associated with the machines' size, and the replacement cost of components. In this regard, some components are statistically prone to failure through handling damage and excessive wear. Such components include memory cartridges and battery backups.

Anno et al., U.S. Patent No. 5,189,288, disclose a method and system for automated voting. Anno et al. describe a computer voting system that utilizes a "Key Card" containing election data to convey vote control to a vote recorder. After use by the voter, the "Key Card" is returned by the voter and the vote data is then recorded from the "Key Card". However, the information in the Anno et al. key card creates undue complexity in the voting process by requiring an added level of supervision.

The designs disclosed in Wise et al., supra, and Webb, U.S. Patent No. 4,774,655, relate to the capacity of available technology to perform voting tabulation. However, the prior designs do not relate to an in-depth scientific analysis of the requirements of public officials, public law, and the provisions necessary for fair, accurate, and secure voting. Also, a means to subsequently verify the system's operation through use of an audit trail with individual voter records or a data difference resolution methodology is lacking.

Obsolescence is also a significant factor that must be considered in the design of electronic voting systems. The manufacturing cycle of state of the art components may make replacement and repair parts unavailable before the end of the system's useful life. As components and technology become obsolete, as in prior art voting machines and system designs, it becomes increasingly important to select technology that is inexpensive, available in quantity, and replaceable with newer components as they become available.

An example of obsolescence is shown by Boram, U.S. Patent No. 4,641,241. Boram discloses the design and use of a voting machine memory cartridge used to remove and store election data. The type of memory described is random access memory (RAM) which requires constant power so that the data is not lost - i.e., volatile memory. A cartridge design is utilized to facilitate handling.

Technology advances and design advances have rapidly advanced since Boram has issued in 1987. Memory technology advances include the development of "Flash Chip" technology.

This memory medium is functionally equivalent to RAM memory data. However, the incorporation of flash memory overcomes a significant potential failure area. In terms of facilitating the ease of handling, flash chips are now packaged in standard business card size modules with an electrical interface. The introduction of flash chip technology demonstrates that it is increasingly important for voting systems to be able to adapt to newer technology.

Prior art systems do not provide for a defined audit trail for the complete operational cycle during an election. The prior art also fails to provide for specifically defined security processes and events that would make security breeches detectable. Moreover, the prior art does not provide for the collection of individual voter records recounting the actual ballots cast.

SUMMARY OF THE INVENTION

The present invention provides a remote electronic voting system which provides improvement over the prior art by simplifying the hardware and software. The present invention is flexible and adaptable (1) through the availability of a single-use design (2) by incorporating defined security protection through both detection and inherent design and (3) by integrating and networking hierarchical systems at the precinct, city/county and/or state levels. Centralized hierarchical control and remote vote recording with secure collection are also provided. A process of immediate election certification by comparison and verification of redundantly recorded data is also provided. Time tagged data and a specific voter record are utilized as disclosed herein. The development and collection of a full audit trail for post election certification is also defined. A methodology of supplying machinery for public elections by defining a single use "kit" concept for certain system elements is disclosed to thereby reduce costs and afford system security.

Also described herein is an electronic "security key card". Unlike the prior art, the security key card is only used to

convey the authority of the card holder to vote. It is (1) issued when the voter's registration is verified, (2) contains a unique code electronically written on a magnetic strip, (3) can only be used one, and (4) is disposable after use. It contains no control data, no election data, nor does it record any vote data. In this case, the prior art is improved by specific simplification of the electronic security key card.

This invention also includes an audit trail and an individual voter record which are specifically defined. Methods employed in this invention, as disclosed, reveal how this critical data is used to assure system integrity and accuracy. Specific data processing techniques are used to produce specifically defined data storage information which is stored with the actual data. These processing techniques produce a storage data header; a digital description of the data; multiple check sums of the stored data and its associated header; and data word parity (a digital description of whether the data word is even or odd). This data storage information ensures that the stored data is true. However, should an error be detected, the error can be corrected through "detect and correct" processing incorporated within the system.

The methodology of processing and storing the critical data of the present system incorporates redundant memories as a defense against catastrophic failures, loss, and/or damage of the transportable memory devices.

A complete system for conducting public elections is disclosed to meet the legal requirements of many jurisdictions and provide secure, centralized, automated vote tabulation. The present system consists of a precinct level system, a city or county level system, and a state level system. The basic system or "precinct system" is a single-use system and is composed of "1 through n" electronic ballots connected to and controlled by a central precinct processor. The precinct system is further connected, controlled, and monitored by other hierarchical systems which may be located at the city/county and/or state levels.

Security of the electronic ballot is controlled by a

disposable electronic security key card which is provided to each voter. With the security card, each voter may gain access to the electronic ballot and cast votes for each electoral race presented. Each security card contains a unique, system-generated access number that can be used only once. This system number is encoded as magnetic information on the security key card. With the present system, the voter may retain the security key card after voting or dispose of it at the polling place.

Control of the electronic ballot(s) is provided by a central precinct processor. The central precinct processor communicates with the electronic ballot through electronic interface circuit(s). Logical input channels and logical output channels (LIC/LOC), contained with the electronic interface circuits, read the votes cast by the voter. The LIC/LOC circuits also control indicators on the electronic ballot to confirm the vote selected. After the voter has completed voting and removed the magnetic key card, the precinct processor records the votes cast in an individual electronic voter record and resets the electronic ballot. The electronic voter record is then used to accurately secure vote tallies and recounts. Like a marked paper ballot, the electronic record is a true record of the votes cast by an individual voter.

The central precinct processor system provides for precinct operator interface and precinct control of the system. The operator can run tests, monitor various system functions, and utilize built in test functions to troubleshoot and repair system and component failures and to also detect security compromises. The central precinct processor also performs communication functions with higher level systems if the installation is so configured. Higher level communication functions may include (1) centralized start and stop commands, (2) system monitoring, (3) data collection, and (4) on-line certification processes. All communications are via encrypted data transmission.

This invention incorporates (1) a single-use precinct system and associated electronic ballots, (2) a higher level

city, county, and/or state level data collection system, (3) a maintenance monitoring facility, (4) associated security provisions, (5) processing to control system functions, (6) a defined audit trail, (7) a defined electronic voter record, (8) system self diagnostics, (9) specific operator displays and displayed data, and (10) processes by which the system is designed manufactured, shipped, installed, and operated. Also included is (1) the method of kit component collection, (2) the delivery of the kit, and (3) the secure handling of sensitive components through the "chain-of-custody" process.

The present invention provides an automated voting system that utilizes electronic components with logical processes and specific security method to provide cost effective, secure collection of votes cast in public elections. The present invention also provides automated vote tabulation and is also adaptable to the specific needs and laws of the jurisdiction in which the system is being used.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a Voting System Block Diagram showing a Functional Allocation of each voting level.

Figure 2 is a Precinct System Diagram.

Figure 3 is a City/County Block Diagram, showing a Remote Recording Electronic (RRE) Configuration.

Figure 4 is a State Block Diagram Remote Recording electronic (RRE) Configuration.

Figure 5 is a Secure Single-Use Voting System Method.

Figure 6 is a Critical Data Processing and Method showing a critical data element and header.

Figure 7 is a Test Valid Critical Data Store Method.

Figure 8 is a Detect and Correct Process Method.

Figure 9 is an Audit Trail Processing Functional Block Diagram.

Figure 9a is an Audit log Post Election Processing Verification Report.

Figure 10 is an Electronic Voter Record and Vote Tally Processing Functions and Method.

Figure 11 is a Security Processing Functional Block Diagram.

Figure 12 is a Statistical Processing Functional Block Diagram.

Figure 13 is an On-Line Maintenance and Monitoring Process Functional Block Diagram.

Figure 14 is a diagram of a Display Format.

Figure 15 is a diagram of Typical System Display.

Figure 16 is a Precinct Hierarchical Display Structure.

Figure 17 is a City/County Hierarchical Display Structure.

Figure 18 is a State Hierarchical Display Structure.

Figure 19 is a System Start Up Screen.

Figure 20 is a System Pre-test.

Figure 21 is a Ready-to-Vote Display.

Figure 22 is a Precinct Status Display.

Figure 23 is a Precinct Statistics Display.

Figure 24 is a Help Status Display.

Figure 25 is a City/County Status Display.

Figure 26 is a City County Statistics Display.

Figure 27 is a Select Precinct Display.

Figure 28 is a County Status Display.

Figure 29 is a District Based Statistics Display.

Figure 30 shows Common Logical Processing Functions.

Figure 31 is a flow chart of Self-Validation Logical Processing.

Figure 32 is a flow chart of Audit Trail Processing.

Figure 33 is a diagram of a Typical Electronic Ballot Layout.

Figure 34 is a diagram of a Rhode Island Sample Ballot.

Figure 35 is a diagram of a Split Ballot.

Figure 36 is a diagram of a Split Ballot with Common Referendum Issues.

Figure 37 is a diagram of a Split Precinct Ballot Configuration.

Figure 38 is a diagram of a Split Precinct System Configuration.

Figure 39 is a Multi-Vote Race Ballot with Vote Counter.

Figure 40 is a Multi-Vote Race with Multi-Votes Per Candidate Allowed.

Figure 41 is a Central Precinct Processor Functional Block Diagram.

Figure 42 is a flow chart of a Stand-Alone Precinct Test Function.

Figure 43 is a flow chart of a Build Valid Precinct.

Figure 44 is a flow chart of a Start Audit Log.

Figure 45 is a flow chart of Run Communications.

Figure 46 is a flow chart of an Establish and Test Communication.

Figure 47 is a flow chart of a Run Memory Test.

Figure 48 is a flow chart of Test Key Card Writers.

Figure 49 is a flow chart of a Test Electronic Ballot.

Figure 50 is a flow chart of a Vote Precinct.

Figure 51 is a flow chart of an Initialize and Verify System.

Figure 52 is a Ready-to-Vote diagram.

Figure 53 is a flow chart of a Run Vote.

Figure 54 is a flow chart of a Record Vote.

Figure 55 is a flow chart of a Validate Key Card.

Figure 56 is a flow chart of Run Ballot n.

Figure 57 is a flow chart of Compile Vote Records.

Figure 58 is a flow chart of an End Vote.

Figure 59 is a flow chart of a Certify Vote.

Figure 60 is a flow chart of a Run Certification Processing.

Figure 61 is a flow chart of an End Precinct.

Figure 62 is a flow chart of Statistics Processing.

Figure 63 is a flow chart of a City/County/State Control Processing Functions.

Figure 64 is a flow chart of a Pre-Election Test Function.

Figure 65 is a flow chart of a Verify Storage and Set Precinct I/O.

Figure 66 is a flow chart of Set Up Precincts and I/O Channels.

Figure 67 is a flow chart of Process Secure Communications.

Figure 68 is a flow chart of Open Communications.

Figure 69 is a flow chart of Collect Pre-Test Data.

Figure 70 is a flow chart of a Certify Pre-Test.

Figure 71 is a flow chart of an Open Polls Command.

Figure 72 is a flow chart of City/County and State Data Collection Processing.

Figure 73 is a flow chart of Run Secure Communications.

Figure 74 is a flow chart of Validate Precinct diagram.

Figure 75 is a flow chart of Collect Vote Data diagram.

Figure 76 is a flow chart of Certify Election diagram.

Figure 77 is a flow chart of Display Election Returns.

Figure 78 is a flow chart of Shutdown Election.

Figure 79 is a flow chart of a City/County Off-Line Data Processing Functional Block.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1, Voting System Block Diagram and Functional Allocation, is a block diagram that discloses the overall system architecture by identifying the system's major components and their major functions. The system functions include: vote collection, data processing and recording, display processing, system control, and other functions. Figure 1 shows an implementation of the complete system as installed. Hierarchical control and recording capabilities from central state locations and monitoring facilities provide centralized operational and maintenance support. The system is organized from the lowest level element, the precinct system, through the state level.

The precinct level is a fully operational, stand alone, direct recording electronic (DRE) voting system. The DRE voting system contains a central processor electronically interfaced to "1 through n" electronic ballots, as shown in Figure 2, Precinct System Diagram. The Precinct System Diagram of Figure 2 shows a dedicated voting system of single use design; i.e., it is intended for use in only one election, after which it is disposed. If the precinct system(s) are connected to a city/county control collection system, the system together is

then defined as a Remote Recording Electronic (RRE) voting system as shown in Figure 1.

The functions performed by the city/county and state processors are dependent on the laws of the jurisdiction. The functions may vary from simple on-line vote collection and performance monitoring to full control of lower level precinct processing. Control functions such as start vote, stop vote, time synchronization and other functions are provided. These functions may be changed, added, or deleted to allow the system to be adapted to the specific voting laws of the community. Figure 3 shows the City/County system in a Remote Recording Electronic (RRE) Configuration.

Figure 4 shows a State System block diagram in the RRE Configuration. Its range of functions are dependent upon the jurisdiction of use. For example, some systems do not require state level tabulation. Accordingly, a state level processor may not be required. However, those states which desire a state level processor can choose the same range of control options available to the city/county processors.

As shown in Figures 3 and 4, those communities using a centralized city/county and/or state processor can opt for electronic information release. Data release options may include on-line statistical data collected throughout the voting period to final election results. Data releases may include a variety of outlets including the news media, various party headquarters, and/or other interested parties.

Security of the system is afforded by a number of features including: data encryption as shown in Figure 1; security key access to the electronic ballot as shown in Figure 2; software self-validation; system handling methodology as shown in Figure 5 and the Secure Single-Use Voting Method System.

An important aspect of this invention is the design of the dedicated precinct system as a "kit" intended for a single-use. The "kit" design relates to a method of providing voting system equipment for a dedicated single-use purpose. The kit design allows all components of the precinct system, as shown in Figure 2, to be common with the exception of the electronic ballots and

the computer program which are tailored for each precinct and election.

This kit design allows all components for all precincts to be centrally pre-positioned prior to an election. To make up a "kit", individual components of the voting system are packaged together and prepared for shipping to the system point of use, i.e., the precinct. Upon arrival at the point of use, the kit is assembled and the full precinct system is ready for the election. After use, the system is disposed of.

The specific methodology is graphically depicted in Figure 5. The inventor(s) have determined cost savings and enhanced security is afforded by the method and the design. Specifically, the following attributes are realized.

Cost Savings

As shown in Figure 5, Secure Singe-Use Voting System Method, the kit design allows centralized warehousing of component parts. Packaging of the kit is performed at shipping time by collecting the system components. The kit is shipped directly to its point of use just prior to the election and assembled. This method yields savings in system assembly, labor, storage, and shipping costs.

After the election, it is contemplated that the system components may be disposed of. It has been determined that equipment handling, storage, maintenance, and reprogramming may, depending upon economic circumstances, be greater than the cost of simply replacing the equipment with new equipment on a per election basis.

Methodology Security

System components are collected randomly and then packaged as kits. Since there is no way of knowing where any specific component will actually be used, tampering with a particular component could not affect a specific election result.

The warehousing method, collection of the kit component parts, and shipping directly to the point of-use is a "chain-of-custody" procedure, as shown in Figure 5. This precludes the

chance of the election equipment being available to unauthorized personnel or potential tamperers. Specific kit components that must be protected are the electronic memory media containing the operational software and the memory where the vote data will be recorded. These components are shipped separately to election officials. The memories are sealed at the time of manufacture and later opened. Only the election officials or the election judges at the precinct may open the memories at the precinct from the sealed package. Multiple identical copies are provided from which the judges make a random selection of the computer program memories. These memories are then installed in the computer. At turn on, security processing is performed by the computer program to validate itself and to assure that tampering has not occurred.

The disposal of the equipment after its use prevents the opportunity for tampering between elections when the equipment would normally be in storage. Since it is contemplated that the equipment may be disposed of, analysis of the system and computer program techniques by a tamperer may be precluded.

Advanced Features of the Invention

Operational and processing advances include:

a. critical data processing and methods;
b. a defined audit trail;
c. a defined individual voter record;
d. defined security processes and operator notification alerts;
e. statistical data collection and real time display;
f. continuous system diagnostic processing; and
g. defined displays.

Critical Data-Processing and Methodology

The critical data collected, processed, and saved or stored during use of the system is the audit trail and the individual voter record data. When combined, it may be determined that the system was properly functioning at the time a vote was cast and

that the vote data is, in truth, what the voter actually selected. The accuracy of this data must be guaranteed and provable to be correct. This is fundamental to the integrity of the system.

Prior art systems have attempted to achieve guaranteed, provable data through redundant memory system data storage. However, redundant data storage alone, without a definitive process to define how differing data is resolved, cannot be proven to be true or accurate.

Multiple memory systems are provided, as shown in Figures 2, 3 and 4, as a defense against catastrophic failure, accidental loss, and/or damage of the memory devices. Accuracy and integrity of the data is assured through the use of data processing techniques that produce specifically defined storage information for the vote and audit trail data.

In reference to Figure 6, Critical Data Processing-Method, these processing techniques produce a Critical Data Element for either a voter record or for an audit trail record (audit log record). The raw data contained within the critical data element will vary in form and content when used as the voter record or the audit trail record. Accordingly, the Data Type, as shown in Figure 6, will indicate the type of information present in the Critical Data Element.

The Critical Data Process is used to add information to the raw (unprocessed) information for each record. The information added to each record includes: a Critical Data Header; a Data Checksum; and a Data Element Checksum. Included within the Critical Data Header is the above-mentioned Data Type which is a digital description of the data type stored. Also included in the Critical Data Header, as described below, is a Time Tag, Number of Words, and word parity information corresponding to each word of the stored data. A Header Checksum is also provided which indicates the number of bits in the Critical Data Header.

Figure 6 also shows the processing performed to produce the critical data header and multiple check sums. When the critical data process is performed to produce a record from the raw data,

it first tests and sets a parity bit for each 8 bit byte of the raw data element. The raw data is then referred to as Record Unique Data. The process then continues and builds the Critical Data Header. The Critical Data Header consists of the Data Type identifier; a Time Tag which is the current real time of the system (a unique number for each Critical Data Element); and a Header checksum. The Header Checksum is a numerical addition of the data in the header with any overflow being ignored.

A second checksum, Data Checksum, is built on the Record Unique Data and utilizes the same process. The Data Checksum is a numerical addition of all bits in the Record Unique Data with any overflow being ignored. The Record Unique Data is simply the raw data which has been processed for parity information as described below in reference to Figure 7.

The final step in the critical data process is to build a third checksum, Critical Data Element Checksum, for the entire Critical Data Element. The Critical Data Element Checksum is a numbered addition of all bits contained within the Critical Data Element. The Critical Data Element checksum is a unique number which incorporates the information from the time tagged number of words.

This combination of header data, parity, and multiple checksums guarantees that the stored data is accurate and true; and, if a data error were to occur, this combination would allow detection of the incorrect data and repair of the incorrect data.

Figure 7, Test Valid Critical Data Store Method, illustrates the use of verification data produced by these processing methods to read and verify the critical data. Each process that reads, stores or otherwise utilizes the critical data within the Critical Data Element checks the verification data record prior to performing any other process. This ensures that the information is correct.

As shown in Figure 7, the Test Valid Critical Data Store process verifies the integrity of the Critical Data Element by regenerating the checksums contained with the Critical Data Element and comparing the result to the checksums generated and

stored by the Critical Data Process of Figure 6. If the checksums are equal, the data is valid and the process is complete. Additionally, the integrity of the information has been verified to be correct. However, if the checksums are not equal, a Detect and Correct process, as outlined below in reference to Figure 8, is performed to find and correct the incorrect data.

Figure 8, Detect and Correct Process Method, shows the processing method performed to correct stored data errors. First, each checksum is tested to identify which part of the critical data element is incorrect. In other words, each checksum including the Header Checksum, the Data Checksum and the Critical Data Element Checksum is recalculated and compared with the stored value in the Critical Data Element. An incorrect match will indicate which portion of the Critical Data Element is in error.

Next, a test of each parity bit corresponding to each byte of data is recalculated and compared with the stored value to determine which byte of data is incorrect. The combination of the checksum and parity information then provides a unique determination of the data bit or bits that are incorrect. The process then "repairs" the data, in a process described below, by setting the incorrect bits to their correct value.

The repair process is shown by the Test Valid Critical Data Store of Figure 7. First, the stored information is read. Next, the parity information for a corrupted byte is analyzed. The parity information for each byte of data will identify which byte has the incorrect data. Each possible combination of bits for the incorrect byte is then sequentially generated and added to the other bytes in the record. The checksum is then recalculated and compared with the stored value. This process is repeated until the value of the added bytes equals the checksum. The incorrect byte is then replaced with the "generated" byte to thereby repair the incorrect byte. This process may be used to repair either the Critical Data Header or Record Unique Data.

Finally, the process generates an audit log record of the

fact that the record was repaired. This feature, incorporated together with the specified voter record content and the methodology used to tally election totals, yields an accurate and secure election system. These techniques are used throughout the system for any process that stores, reads, or uses critical data.

This method assures the accuracy of the critical data elements produced by this invention, the audit trail, and the individual voter record.

Audit Trail

Security and credibility are key issues that must be accommodated by an automated voting system. To facilitate these issues this invention includes a specific audit trail that is continuously updated and records each system event in a time ordered sequence. Audit trail data is critical data and incorporates the critical data process methods previously defined. Event data is produced by each major processing function and a specified data record is also produced that fully describes the event. This data is redundantly stored in multiple data memories.

Figure 9, Audit Trail Processing Functional Block Diagram, illustrates the production of data by each major processing function and shows the data logged. The data provided is such that the complete operation of the system can be reproduced and the system's operation confirmed. This audit trail and the data included for each audit log entry in the audit trail are defined below:

A. Time of log entry
B. Time of event occurrence
C. Event category
    1.) System Turn On
    2.) Ballot Access
    3.) Ballot end Access
    4.) Vote Entry, Vote Confirmation Commanded
    5.) Operator Entry
    6.) Maintenance Monitor Entry

7.) Failure Detection Process
8.) On-Line Manual Test
9.) State Voter Record
10.) Pre-election Test Record
11.) Start Vote
12.) End Vote
13.) Certify Vote
14.) Security Alert
15.) Power Failure
16.) System Restart
17.) Commands
18.) Communication Processes
19.) Voter Help Processes
20.) System Shut Down Command

The data sets, which comprise the audit trail, can be used to completely reproduce all events which occur during the voting day. This audit trail can be thoroughly reviewed after the election through off-line processing. The availability of the audit trail allows the reproduction of all system events. This validates the operational integrity of the system during its operation and satisfies the necessity to demonstrate system credibility.

Processes that utilize this data would most probably be specifically defined by either a procedural specification to establish the system operation after an election or a specific event that necessitated an operational reconstruction. In any event, the uses of this data in post election processes are numerous. However, by way of example, a post election validation process is provided.

By way of example, and in reference to Figure 9a, a post election validation process is provided. For this example, the specification is that the operation of the system is to be confirmed over a 30 minute time frame from 10:00 a.m. to 10:30 a.m.

To perform this, a specific procedure would read all of the audit log entries that were processed over that time frame and provide a printout of the audit log data. Figure 9a is an

illustration of how this printout of the audit log data might look. Verification utilizing this data could be performed by a human review of the data.

Individual Voter Records

The present invention defines an individual voter record to ensure secure, accurate and true election results. This is as shown in Figure 10, Electronic Voter Record and Vote Tally Processing Functions and Method. The voter record is an electronic record of the ballot as cast by the voter i.e., a digital record of those votes cast by an individual voter. The individual voter record is an element of the system critical data and uses the critical data processes and methodologies previously defined. It is this record from which the totals of each electoral race are derived. The voter record is the electronic equivalent of a marked paper ballot. Each voter record is saved and can be used for later recounts. It can be printed off-line and manually recounted if necessary. The system does not merely provide vote totals of each race, but rather a complete voter record for each voter from which vote tallies are compiled. Each individual's votes can be clearly understood after the polls are closed. This allows for a meaningful recount and is used to verify that the software logic that correlates the voter's choices to the vote cast is correct. If for any reasons such logic was incorrect, it then could be subsequently corrected and recounted. This is not possible in a system that saves only the total votes cast in each race.

Security and accuracy are provided by the check sums created and stored with the voter record by the critical data processing functions. These check sums will result in an immediate security breach detection should any part of the voter record be tampered with. The critical data processes not only allow the tamped vote to be detected, but also allow the tampered vote to be changed back to the correct vote. This is an improvement over paper ballots in which an altered ballot may go undetected. If an alteration is detected on a paper ballot, it may not be possible to determine the voter's intent.

As a final security and accuracy check, a vote tallying

process is incorporated in which two or more separate processes tally the votes. These separate processes produce a tally of each race from the voter records. These are then compared, and if equal, would result in a certified election result. The purpose of this method is to ensure that the vote tally process has no logical errors that could cause an incorrect election tally and eliminates human error as a source. In practice, the two or more tally procedures would be developed by different persons to ensure that while the tally function is the same, the actual logical processing would be different. This method eliminates the possibility of logical errors going undetected. The vote record process and method provides additional system security since votes are tallied from these records. A system that maintains a running total could be subject to fraud by tampering if the vote totals were adjusted. To effectively tamper with this system, each vote in each voter record would have to be found and individually adjusted. This is a near impossible task since many copies of each record are maintained throughout the system and each contains unique check sums and parity data as generated by the previously described critical data process and method. Additional protection of the critical vote record data is afforded through the use of separate memory systems and/or devices that contain redundant copies of the voter record and other system critical data.

Security

Defined security processing is fundamental to the design of this invention. Methods employed to monitor security include specific detection processing functions, statistical detection processing functions, and alert processing functions for displays to notify election officials. Figure 11, Security Processing Functional Block Diagram, depicts the processing defined for the security function and includes the operator's required inputs in response to a security alert. Each occurrence of a detected security breach or suspected security breach is logged in the audit trail and the appropriate operation level (precinct, city, county or State) is required to

enter an alert response that becomes part of the operational audit trail.

Security breaches are classified as one of three security alert levels:

Level 1 Alert:

An overt attempt to breach security has been detected and requires an immediate official investigation and response. All levels are notified.

Conditions generating a **Level 1** alert are:

1. Wrong code received on communications line.
2. Communications call received outside of call back time parameter
3. Encryption data incorrect
4. Wire tap detected
5. Computer program self-validation fails
6. Ballot interface codes incorrect
7. Real time data verification fails
8. Vote entry time before/after polls open
9. Voter Record check sum fails

Level 2 Alert:

A potential breach of security has been detected which requires a local official investigation.

If tampering is suspected or proven, the next higher official element is notified and must acknowledge notification.

Conditions generating a **Level 2** alert are:

1. Ballot key code previously used
2. Electronic ballot failure while voter is in booth
3. Failure of ballot interface
4. Power interruption to system
5. Communications reconnect failure

Level 3 Alert:

A statistical condition exists that has generated a security alert and must be locally investigated. If a breach is confined, the next high official element is notified.

Conditions generating a Level 3 alert are:

1. Electronic key card issued but not used after a predetermined time
2. Voter throughout exceeding predetermined level or precinct historical throughput of the day
3. Several voters exceeding average time to vote
4. Number of voters exceeds number of registered voters

Each of these security alerts generate immediate operator alarms. The specifics of the security alert are displayed on the system operator's display.

Statistical Data Processing and Methods

An advancement in this voting system is the definition, collection, processing, and display of statistical real time data. Figure 12, Statistical Processing Function Block Diagram, shows the processing performed by each of the full system hierarchical elements and the statistical information provided at each level. When possible and appropriate, statistical ranges, means, modes, and averages are provided by this function.

Specifically the following statistical information is collected and displayed.

A. Precinct Level:

1. Total number of precinct registered voters
2. Total number of voters and by party
3. Total number of ballot voting stations
4. Voter throughput total, by each hour, and during last hour
5. Average time to vote and range
6. Number of help requests
7. Average help time and range
8. Number of poll workers
9. Total time poll open
10. Lost time due to problems
11. Number of security alerts

12. Election results
    -By office, candidate's name, and number of votes
13. Wait time estimation

B. City/County Level:
1. Same statistics as the precinct except totaled for an entire city or county
2. All of the above is displayed on a precinct by precinct basis
3. Operational status and number of voters by
   a. Legislative District
   b. Congressional District
   c. Council District
   d. Precinct District

C. State Level:
1. Same statistics as city county level except totaled for the entire state
2. All of the above is displayed on a county by county or city by city basis
3. Operational status and number of voters by
   a. Legislative District
   b. Congressional District
   c. Council District
   d. Precinct District

The value of this on-line real time statistical data accrues to both election officials and the general public alike. Election officials can monitor the election to determine if a precinct is becoming crowded. This may allow them to shift added help from a slow precinct to one that has many voters arriving in a short period. Research has shown that definite community trends exist for preferences to vote before or after work or at other specific times of the day. Assessment of the statistical data can allow officials to tailor precinct voting systems and poll workers support to times that trends indicate

are heavy. Public release of this information can also be provided throughout the voting day to allow voters a better choice of when to vote. As a result, a better level of service is provided.

On-Line Diagnostic, Maintenance, Monitoring Processing

The ability to continuously prove that the system is operating as required and to quickly detect, find, and fix any failure of the system are afforded through on-line continuous diagnostic maintenance, and monitoring processing functions. This functional process is shown in Figure 13, On-Line Maintenance & Monitoring Process Functional Block Diagram. Functions in this process include "Find and Fix Processing" to aid the system operator in repairing any failure to minimize the voting minutes lost.

"Find and Fix Processing" is a continuous process that "repairs" problems of selected hardware components and logical processes incorporated in the system. These include interface word parity, bit detect, correct circuitry, as well as other processes. Other processes include check sum validation, test words and other continuous monitoring, and diagnostic testing. Fault Detection and Correction performed in these processes are termed "Soft Failures", i.e., a failure that could be corrected by the functions performed by the hardware and software of the system. When fault detection is reported through a scheduled run of the on-line maintenance, it is used to develop a statistical report that can be used to assess the overall "operational health" of the system, e.g., the number of communication line faults detected and corrected. By way of example, a 25 percent communication detect and correct fault rate may prove to be common and acceptable while a 50 percent rate may be determined to be enough degradation to warrant repair procedures.

In further reference to Figure 13, the present invention accounts for hard failures. Hard failures are failures that cannot be fixed through the incorporated process, e.g., a complete loss of communication. In this case the "on-line

maintenance monitor function" immediately processes to determine the fault, reports the fault on the system operator's display, and performs processes to localize the failed item. The Find and Fix function of this process determines which component has failed and reports this to the operator via the maintenance monitoring operator display function. This will provide the operator assistance in repairing the system.

Periodic fault detection is one of the functions performed by the election operational computer program and includes processes for both hard and soft fault detection and operator notification. Periodic testing includes verification of interfaces, ballot channel testing, communications test messages, and lamp tests.

Operator display processing functions include fault display processes, fault alert display processes, specific operator instructions to fix system, and monitoring statistical processing functions.

Results of all of these maintenance and monitoring processes are saved as part of the system audit trail. During a post election analysis, not only can events be verified, but the operational status of the system before, during, and after a particular event can be confirmed.

System Displays

Displays at all levels of the system are significant to the present invention. The overall format for these displays is shown in Figure 14, Display Format. The purpose of displays is to provide a logical operator interface to allow operational functions to be performed. The displays are specific and logically organized to limit the range of operator actions required to direct the system's operations.

Physical manifestations of these displays may include color, "point and click" methodology, and other useful techniques. However, the defined operator actions and data displays are more important to the present invention.

The System Display area is common to all displays and is used to display legally required data such as public count and

precinct number.

The Alert Display area is specifically reserved for operator alerts such as security alert and maintenance alert.

The center area of the screen is a Selectable Data Display area. Data displayed in this area is selected by the operator.

The Function Key Display area, at the bottom part of the screen, is used to display function key switches that can be accessed from a particular display and are changeable from display to display. These are known as "soft keys" i.e., keys whose functions are changeable by the computer program.

The preferred embodiment of this display design incorporates the man-machine interface of the common "point and click" method. The displays may incorporate the use of colors and other features commonly available to enhance the utility of the displays.

System Display Area

Common elements displayed in the system area may be fixed and determined by the laws of the jurisdiction of use. These are typically displayed when the system is operational as shown in Figure 15, Typical System Display. Displayed elements include:

1. Public Count
2. Precinct Number, City/County, or State
3. Time Data
4. System Status
5. Poll Status

Color usage in this display may include the following background colors for the "Booth Operational" display.

Green: Operational

Red: Down or failed

Yellow: A help alert has been processed. Operator can return square to green with "point and click" or system will reset to green when voter is done.

Alert Area

This area is reserved specifically for the operator alert display area as shown in Figure 15.

Alerts displayed include the following:

A. *Security Alerts*
   1. Type of Security Alert
   2. Time of Alert
   3. Necessary Action

B. *Maintenance Alerts*
   1. Type of Maintenance Alert
   2. Necessary Action

C. *Procedural Alerts*
   1. On-Line Test Ballot
   2. On-Line Test Card Writer/Readers
   3. Time to Open Poll
   4. Time to Close Poll

D. *Command Alerts*
   1. Contact Message
   2. Open Poll
   3. Close Poll
   4. Estimate Voters Waiting
   5. System Shut Down

E. *Voter Help Alerts*
   1. For example, a voter in booth "n" has requested help.

In addition to the fixed alert data displayed, a set of alert control software switches are provided in a fixed area at the bottom of the alert area. Use of these switches are:

1. HIPRI (Highest Priority)
   - Display highest priority active alert
2. HELP
   - Display active help alert list
3. NEXT
   - Display next alert in active alert list
4. LAST
   - Display previous alert in active alert list
5. REMOVE ALERT
   - Delete the displayed alert from the above list

6. HISTORY

- Display alerts from alert history list instead of the active list

Selectable Data Display Area

This area displays data as selected by the system operator.

Display Function Key Area

The display function key area is reserved for the display of point and click soft switches, i.e., keys whose functions vary depending upon the display and are defined by the software.

Display Structure

Figure 16, Precinct Hierarchical Display Structure, illustrates the hierarchical nature of the display processing organization. At start-up, the available screens, in sequence, are the start-up screen, pre-test and ready-to-vote screens. Figure 17, City/County Hierarchical Display Structure, and Figure 18, State Hierarchical Display Structure, show the display structures at the city/county and state levels.

Once the poll is open and in voting status, all screens under "operational screens" are available to the operator. When a time period designated as "close polls" time is exceeded, a poll closing screen becomes available. This screen allows an operator to provide an estimated time to close the polls. This data is then transmitted to the next higher level system, if they are connected. It also provides a screen for local operator shut down of the polls' voting status. Once this occurs, the operator cannot return to any higher level screen. During certification and shut down processing, no operator inputs can be performed except for log entries.

Figures 19 through 29 illustrate various display screens implemented with this specific design. Note that the return key and log entry key are always shown. A gray background behind a key indicates that it is not available for operator entry. Other methods may be used to actually implement this function. The return key is used to return the screen displayed to the

next higher level of display as shown in Figure 19. This display design, and the data processed and displayed on these specific screens, are unique attributes and specific improvements of this invention.

Logical Processing Functions

Logical processing functions are significant to the present invention. A separate *stand alone test function* is used to verify the full system operation prior to an election. A separate *operational election processing function* used to actually operate and control the system during the election.

At the city/county and state levels, a third *off-line data processing function is* provided. The processing performed by this function provides for a number of post election processes including recount processing, voter record printing and analysis, audit trail review and other processes that may be required by local laws. The post election process is tailored for each jurisdiction.

Common Logical Processing Functions—Detailed Description

Functions common to all logical processing are The Self-Validation Function and the Audit Trail Function. The incorporation of these functions is shown in Figure 30, Common Logical Processing Functions. The Self-Validation processes are performed at system turn on as part of the system's start-up processing and periodically on a continuous periodic schedule. Audit trail processing functions are performed as scheduled by other systems processing functions.

Self-Validation Function

As stated above, the Self-Validation Function is *common to all logical processes* utilized and is shown in Figure 31, Self-Validation Function. Its purpose is to ensure that each process may validate itself at run time and prove that it has not been tampered with. Additionally, the Self-Validation process ensures that no data has been lost through any type of failure.

Specifically, at the time of manufacture, a check sum is

generated and stored with the logical processing command set, i.e., the program. The check sum is an overflow ignored, sequential addition of each command comprising the entire functional process. This number is then added to a security code number to produce a final program check sum.

This produces a completely unique number for each set of logical processing commands. As shown in Figure 31, the run time processing generates a calculated check sum. It is then compared with the checksum stored at the time of manufacturing. A fault occurs if they do not compare. This fault would cause the generation of a level 1 alert which signals that intentional tampering has been detected. Self-validation is run at system start-up, periodically during system operation, anytime the system is stopped and restarted, and anytime a fault condition is detected. This effectively precludes any direct tampering with the logical processing command set.

As an *additional security* provision, a manually entered security code is entered by the operator. This code is added to the calculated code and checked against the stored checksum to validate that system operation is authorized. Failure of this check would also generate a level 1 alert.

Audit Trail Logical Processing Function

The audit trail is a significant improvement in the art and is preferably common to all system processing functions. The processing that generates the audit trail is shown in Figure 32, Audit Trail Processing. The audit trail is developed and recorded by the process Audit Log. *The audit trail will allow every system event to be tracked after the election through off-line processing.*

Specifically, the audit trail is a time ordered digital recording of each system event that occurred during the election. A system event includes: (1) system start time, (2) operator commands, (3) test results, (4) start vote, (5) key card number issued, (6) key card number used, (7) electronic ballot input data, (8) voter start vote and stop vote time, and (9) external commands from higher level elements if they are

used. Additionally all required operator inputs, such as system alert and failure detection responses, are logged.

Each major procedure in the present system uses an audit log procedure to schedule an audit record processing function. When combined with the voter records, a complete audit of every precinct event may thereby be reproduced. The operational integrity of the system can also be verified and validated by an analysis of operating historical records contained in the Audit Trail.

Precinct System Detailed Description

Figure 2, Precinct System Diagram, is a block diagram of the single-use precinct system. As shown, its major components consist of: (1) electronic ballots, (2) an electronic ballot interface, (3) a central precinct processor, (4) magnetic key card writers, (5) magnetic key card readers, (6) external communication components, (7) an operator control station, and (8) provisions for a separate memory media. The separate memory media contains operational logical processing functions and several redundant memories for recording vote data, system operation data, the audit trail and individual voter records. The memory media used for implementation of this invention may be any number of potential media including both volatile and non-volatile media. Examples include flash chips, Programmable Read Only Memory (PROM), laser discs, or industry standard Personal Computer Memory Card International Association (PCMCIA) technology.

All control and data processing functions of the precinct system are performed by a central precinct processor and its associated logical processing functions. Functions performed include (1) overall operational control, (2) pre-election testing, (3) continuous diagnostic monitoring, (4) security monitoring, (5) electronic ballot control, (6) vote data collection, (7) audit trail data collection, (8) secure data communications, (9) time synchronization, and (10) operator interface display processing functions. The logical processing also builds and stores individual voter records, which are the

functional equivalent of a paper ballot and necessary for election certification and recounts.

The precinct system is the lowest level of the *hierarchical design*. The precinct system can be operated as a total stand alone system autonomously operating under its own logical processing control and collecting voter inputs or it may be connected to a higher level system at the city/county and/or state level. Precinct level functions controlled from the higher level system are determined by the community in which the system is being used.

Precinct System Hardware Components

Electronic Ballot

A significant feature of this invention is the electronic ballot as shown in Figure 33, Typical Electronic Ballot Layout. The electronic ballots are shown in a single-use designs manufactured specifically for a particular election. A main feature of this method is that the ballot has no restrictions for the design and layout of its face. It is designed new for every election and for each area of use. Thus, it can be tailored to any jurisdiction's unique requirements. It is representative of a "full face ballot".

Presently, the technology used for the preferred embodiment of this design is *membrane switch technology*. This technology is flexible and cost effective to implement in a single-use design. This technology may also be replaced as newer technology becomes available at cost and in quantity for future systems. The specific design of the electronic ballot allows for all possibilities of voting including straight party voting, write-in voting and multi-vote races. *"Tactile feel"* of vote selection is provided by incorporating dome switches on the electronic ballot. Corresponding system vote selection is confirmed by illuminating a light emitting *device that indicates the voter's selection(s) on the ballot face*. Provisions are also made for *write-in selection*. In the ballot depicted in Figure 33, the write-in provision is provided by an alphabetic keyboard with an associated display. In future systems, this

may be changed to a touch sensitive screen where the voter may actually write in the vote. As this technology matures it will become less expensive and more accurate. Accordingly, incorporation may be provided on a cost effective basis.

Another major feature of the single-use electronic ballot is the ability to design the face for each election without the ballot's physical limitations obstructing the presentation of the information. *Presentation of data* on the ballot can be distinct, providing party affiliation, as well as segregating party affiliation. Color and physical separation of issues without limitation can be used to clearly present the election choices to the voter. Figure 34, Rhode Island Sample Ballot, shows an implementation of an electronic ballot. It is a *"full face ballot"* which can contain multiple languages including embossed Braille and/or candidate photos.

The electronic ballot disclosed herein also provides a *significant enhancement in system security*. Election data on the ballot is applied at the time of manufacturing. It is therefore *physically integral* to the ballots' materials and cannot be tampered with. Any attempt to change the data would be immediately detectable by simple visual inspection as attempted tampering would result in obvious damage to the ballot. Unlike other prior art designs intended for use in several elections, the single-use design, manufactured for only one election, does not have unused switches available to the voter. Such switches could lead to sophisticated tampering through either modification of the computer software to detect an unused switch or by moving the label associated with a given switch. Both unintentional and intentional ballot tampering are eliminated by this method.

The final security provision of the electronic ballot is afforded by the *chain-of-custody method of handling*, as shown on Figure 5, Secure Single Use Voting System Method. The chain of custody method of handling precludes and prevents unauthorized access to the ballot prior to an election.

The electronic ballot affords the following specific improvements on the state of the art.

(1) The ballot can meet exactly the appearance requirements of the law and is adaptable on a per election basis.

(2) There are no row and column limitations, type size limitations, and the layout can contain logical, graphically identified separations to indicate different races, issues and political parties.

(3) The names and issues are imprinted on the ballot during manufacture and are integral to the ballot (i.e.; laminated and/or printed into the materials during the manufacturing process). There is no opportunity for ballot tampering by moving names around on the ballot face.

(4) Since the ballot is specifically manufactured for a particular election, the only switches that are applied, and therefore available on the ballot face, are the ones where a vote is allowed. Therefore a collusion could not occur where an unused or "phantom" switch is used to record additional secret votes through tampering with the software.

(5) Actual candidate pictures and flags representing party affiliation could be incorporated as part of the ballot data.

(6) Embossed Braille could be incorporated as part of the ballot data.

(7) The single-use design requires no additional life cycle costs after the election.

(8) Any number of ballots may be used at the precinct. For general elections a write-in ballot is provided.

The electronic ballot of this invention affords this function through the use of an alphabet keyboard with a display. Current implementation of this function may use a liquid crystal display. Alternatively, software may be used to read handwriting along with a touch sensitive screen where the voter could actually write in, rather than type-in, the candidate of choice.

Access by the voter to the electronic ballot is afforded

through the insertion of an electronic security key card. This key card contains a unique security code generated by the processing functions of the central precinct processor. When the key card is inserted into the electronic ballot, the central precinct computer checks to ensure that the code is currently valid. If it is, the ballot displays a "PLEASE VOTE" and the voter can begin making his/her selections. When the voter has completed making all selections, the key card is removed and the computer resets the ballot to quiescence and records the votes.

A particular specific improvement of the electronic ballot design is the *incorporation of a "HELP" button* as shown in Figures 33 and 34. When the voter depresses this button, an alert will be received by the system operator that a voter using ballot "n" requires assistance. This effectively eliminates the current limitations of several voting machine designs where additional poll workers have to be stationed at each machine or the voter must otherwise attract attention to himself in order to receive help while in the booth. Present state of the art designs in actual use have caused mis-votes due to their lack of this "help" provision.

Another improvement of this electronic ballot design over others is its fixed face that does not require voter control, such as paging through a number of interactive displays, to complete the voting. All election information is displayed "full face". The only voter action required is to depress a button that corresponds to the vote to be cast. Indicator lights, such as LEDs, confirm the selection made. Computer program control of the lights allows vote changes to be made by the voter until voting is complete. Removal of the voter's electronic security key card causes the votes to be recorded.

Another advanced feature of the electronic ballot is the incorporation of a ballot **"RESET"** button as shown on Figure 33. This allows the voter to reset the entire ballot and start voting again without casting the ballot. Note that the ballot is cast once the electronic security key card is removed which is the last step in the voter's act of voting. This is a useful

attribute to the voter and will help minimize voter confusion while in the booth.

The method of access to the ballot, the availability of the "HELP" and "RESET" buttons, and the method of casting the ballot by removing the access key card are all included to aid the voter.

The system computer program and the single use electronic ballot allow for a wide range of voting options to be employed. As illustrated in Figures 33, Typical Electronic Ballot Layout and Figure 34, Rhode Island Sample Ballot, a wide range of candidates, parties, races and referendum issues may be accommodated for a general election. As shown in these Figures, accommodations are made for the selection of write-in votes, straight party voting, and individual candidate voting.

Other ballot styles that can be accommodated by this combination of computer program and a single use ballot include the ballot styles used in primary elections. For these elections a jurisdiction may select a number of options as illustrated in Figures 35 through 40. These include a split ballot as shown in Figure 35; a split ballot with common referendum issues as shown in Figure 36; a split precinct ballot configuration as shown in Figure 37; or separate precinct systems as shown in Figure 38. Voter access to the appropriate side of the split ballot and/or the appropriate ballot of a split precinct is controlled by the issue of a party electronic access key card at the registration table. The computer program used to read the party code only allows votes to be entered on the side of the ballot that corresponds to the voter's registered party. In the case of the split precinct option or the separate system options, the key card can only be used to cast votes on the appropriate party ballot. The provision for write-in candidates is generally not required for primary elections.

A particular election related problem addressed by this invention is the issue of over voting and under voting in multi-vote races where the voter is instructed to "vote for no more than "X" number of the below candidates". The electronic ballot

and its associated computer program totally alleviate the problem of over voting by not allowing the voter to cast votes for more than "X" number candidates.

Under voting is when a voter does not cast all his allotted votes for a race. The voter simply may not have desired to vote the full selection available. To improve the chances that the voter will cast the full allotment of votes available, the electronic ballot can incorporate a counter to provide positive feedback to the voter on the number of votes cast. Figure 39, Multi-vote Race Ballot with Vote Counter, illustrates a potential embodiment of this part of the invention. As shown, a counter indicates to the voter the number of votes cast for the multi-vote race.

Due to the single use ballot and its associated processing and control functions, a particular voting methodology is provided for the multi-vote races where the voter may cast one, or more, or all of his allocated votes in the race for one candidate. Figure 40, Multi-vote Race with Multi-votes Per Candidate Allowed, illustrates how this would be implemented on the electronic ballot. The use of the multi-vote counter and the vote indicator lights are improvements manifested by the flexibility of this invention.

Over voting is eliminated by this system simply because the system will not accept more votes to be cast than allowed in the multi-vote race. Under voting cannot be controlled in such a positive manner because the voter may not desire to cast all of the allowed votes. It is intended that the use of the multi-vote counter, the multi-vote race layout of the electronic ballot, and the incorporation of light indicators will improve the opportunity for a voter to understand the number of votes available. This innovation is a general improvement on the overall state of the art.

The interface between the electronic ballots and the central precinct computer is provided by interface circuits which provide the logic necessary to read the voter's switch actions, light the associated vote indicator lights, and convert logical data to digital data for interface with the precinct

processor. The precinct may contain any number of electronic ballots. The interface circuitry also provides all power required by the electronic ballots. This is an important safety improvement over the prior art. At the ballot, the only electrical current is low voltage direct current (DC) power. Therefore, the risk of accidental shock to a voter is significantly reduced.

Central Precinct Processor

Another major component of the single-use precinct system is the central precinct processor (CPP). Like the electronic ballot, the CPP is afforded tamper resistance, both physically by its inherent design, and methodically through its single-use kit design and chain-of-custody handling.

Figure 41, CPP Functional Block Diagram, shows the functions performed by the CPP. The physical manifestation of this invention would presently have these functions performed by a general purpose digital computer and an associated single purpose computer program that contains the processor commands necessary to perform the CPP functions. Physical manifestations of this invention may also use special purpose data processors, integrated circuits, or other technology to perform the logical processing functions allocated to the CPP.

The functions performed by the CPP include (1) continuous system testing and performance monitoring, (2) security monitoring, (3) magnetic security key card writing and validating, (4) electronic ballot control, (5) redundant data storage, (6) audit trail processing and storage, (7) voter record processing and storage, (8) operator interface processing, (9) election certification processing, (10) secure communications processing, and (11) statistical data processing.

When the precinct system is interfaced to a higher level city/county and/or state system, it will also perform the communications functions necessary to allow the level of control specified by the user community.

The data storage function or memory, the specific design features of this invention, and the methodology of handling the

memory medium itself before, during, and after the election are methods implemented to assure the fairness, integrity, accuracy, and tamper resistance of the election data.

The design of the operational vote memory system and its chain-of-custody handling are also basic aspects of security afforded by this invention. It is contemplated that the physical implementation of the memory system will change as new technology affords advancement. Current technology, such as Personal Computer Memory Card International Association (PCMCIA) technology, is the preferred physical embodiment of the memory system. Other advances may well evolve over the life of this patent that improve the physical implementation of the memory system, but the required functions will remain the same, i.e., redundant and separate records of the election.

Once the precinct kit is assembled into a system at its point of use, it is tested using a *stand alone test function*. The test verifies the operation of all system components, including the correct operation of all electronic ballot switches, and confirms that the switch action is associated with the candidate issue shown on the ballot. This data is saved on the test memory medium by audit trail processing. Both the test functional processing and the stored test results are then saved for post election analysis. The operational election functional processing is provided by the system supplier. This function is developed and tested specifically for each individual election and is part of the single-use design of the entire precinct system. Multiple copies or memories bearing duplicate functional processing commands are supplied for each precinct. The final step of the manufacturing process is a comparison of the functional processing commands on each of the memories to ensure that the correct command set is installed and that the commands have been transferred to the memories correctly. Once this verification has been performed, the multiple memories are placed in a sealed shipping container for shipment directly to the precinct of use. The sealed container is then opened by election judges at the precinct. A random selection is then made by the election judges and installed in

the CPP.

When the system is energized, a *self-validation* logical process function will be performed, as shown in Figure 31, to ensure that the logical processing command set has not been tampered with. A human controlled check will also verify the correct command set is installed. The system will display precinct information on the operator's display. The system operator will then confirm that the displayed precinct information is correct.

This methodology assures the correct logical processing functions are in use, and that tampering, changing or failure of the logical processing command set has not occurred. In addition, this methodology it verifies the chain-of-custody from manufacture to use.

The electronic security key card system is provided to allow only authorized voter access to the electronic ballot. This precludes the need for a polling official to be stationed at each booth to control ballot access.

The logical processing functions of the central precinct processor generates the unique code that is magnetically written onto a magnetic strip of the electronic security key card. The code is generated when a registration worker requests the key card. The logical processing function that writes the code also reads back the code from the card to ensure that the correct code was written on the magnetic strip. The key card is then given to the voter.

The voter takes the key card to the voting booth and inserts the key card into the electronic ballot's key card reader. The logical processing function validates the key card as "authorized to vote" and sets the electronic ballot to accept the voter's selections. Once the voter has completed his selections, the key card is removed and the vote is cast and recorded.

Precinct Logical Processing Functions

Two logical processing functions are provided for the precinct system. They are the Stand-Alone Test and the

Operational Vote logical processing functions.

Stand Alone Precinct Test

The purpose of the stand alone pre-election test is to ensure that all system functions, and components are operational. The results of this test are saved. The stand alone test is tailored to suit the actual precinct operational environment. If the precinct is connected to a higher level system, all functions that are specified for higher level communications, as well as control functions, are validated by this test.

Figure 42, Stand Alone Precinct Test, depicts the stand alone precinct test using standard structure flow charts. A detailed description of this processing follows.

The first processing function performed by the computer program is self-validation. This confirms that no tampering has occurred in the logical processing command set. This process is shown in Figure 15. Processing is then performed to initialize the operator's display and prepare it to receive data. It also establishes the interface processing necessary to receive operator inputs from the operator's keyboard. This processing will also test that the operator's display device and input keyboard are operational.

The logical processing function then validates that it is appropriate for the precinct in which it is being used. This requires an operator's input. Detailed processing of the build valid precinct processing is shown on Figure 43, Build Valid Precinct. As shown, a primary piece of data input to this process is the system adaptation table. This allows one logical processing function command set to be designed to operate on several differently configured systems and reduces the overall cost of the system. The adaptation table is a run time parameter that directs the processes being performed so that the processing will comply with the specification of the individual system. A typical set of adaptation parameters is shown in the ST ADAPTABLE on Figure 43, Build Valid Precinct. This configuration of the adaptation table describes processing for

a fully implemented hierarchically controlled precinct. For jurisdiction designs that do not have a full hierarchical control element, the adaptation parameters are changed to modify the precinct processing so that such functions are not performed. The build valid precinct processing, shown in Figure 43, is processing that asks for the operator to enter the precinct number. The valid precinct number is read from the adaptation parameter table and compared with the operator entered precinct number. If they match, the valid precinct code is set true and stored for use by other processing. System operation then continues.

The next process performed is the audit log start up processing. Detailed processing is shown in Figure 44, Start Audit Log, and Figure 16. This process clears and tests its reserved memory area. If it verifies all zeros, the audit log stores all system start up parameters.

Further processing performed by the stand alone precinct testing validates the operation of all system components and logs all test results in the audit log table. The detailed processing is shown in Figures 43 through 49. All procedures executed by this process conclude with the audit log process. It is this process which generates the audit trail.

The communications hardware connection and data processes are validated by the Run Communications procedure shown in Figure 45 and the Test Communication procedure shown in Figure 46. All memories are tested to ensure that data can be read and written into them as shown in Figure 47. Security key card writer/readers are tested as shown on Figure 48. All electronic ballot interface and control functions are tested as shown in Figure 49.

Operational Election Logical Processing Function

The purpose of the Operational Election Logical Processing Function is to perform functions through its operation that provides for the secure and accurate collection of votes and the tallying of votes for each electoral race.

The detailed processing functions performed by the

operational precinct logical processing functions are shown in Figure 50, Vote Precinct. When the system is energized, it first validates itself as shown in Figure 31. This confirms that no tampering has occurred in the logical processing functions.

The initialization and verification of the system is performed as shown on Figure 51, Initialize and Verify System. This processing initializes the display console, and validates the precinct as previously described in the stand alone precinct test, as shown in Figure 42. It then reads, verifies, and stores this data in the audit log. The next function zeros all recording memories and verifies the zero recording. This processing also directly tests the memories as well. The initialization processing also establishes communication to the next higher level system if it is specified in the adaptation table. During the initialization processing, data provided by the precinct processor includes precinct test results, time synchronization, and precinct status. The final processing performed in initialization is a system test. *This test is a statistically significant subset of the test performed by the pre-election stand alone test function and verifies that all system components are operational.* Test conduct and results are saved in the audit trail and also sent to the next higher level, if it is present.

Once the initialization and verification processing is completed, the system begins the "ready to vote" process. This processing is shown in Figure 52, Ready To Vote. The first processing performed displays the current vote count and public count of the system. At this time, these displays should display zero (0). This processing cycles until real time is greater than or equal to voting start time and the start vote command is set by the system operator as approved by the precinct election judge. See Figure 52.

The run vote processing is shown in Figure 53, Run Vote. The first processing performed is the "allow interrupts procedure". This procedure allows the system to change from the quiescent stage of "ready to vote" in which all electronic

ballot and key card inputs are logically locked out to the operational status of vote.

The record votes procedure is depicted in Figure 54, Record Vote. Functional processing is performed to validate the voter's key code. The key code verification is shown on Figure 55, Validate Key Card. This processing function checks the valid code table. If it is valid, the process writes the code in the voter record. If it is not a valid code, security processing is performed and an operator alert display is generated.

The second process performed in record vote is "run ballot" and is shown in Figure 56 as "Run Ballot n". This processing reads the voter's input from the electronic ballot interface buffer. The vote input is then logged.

The final process performed by the record vote process is to determine if the cast ballot flag is set. If it is, the critical data process is run to produce the voter record header, checksum, and parity data. The voter record is then stored and validated in the redundant memories.

The "compile vote records" process continuously tallies the totals for each candidate and issue. This processing is shown in Figure 57, Compile Vote Records.

When the "end vote" command is received from the system operator and real time is greater than or equal to the end vote time, the system begins "end vote" processing. This process is shown in Figure 58, End Vote. This process locks out all electronic ballot interrupts and calculates the last vote totals.

The final process performed at the precinct is "election certification" as shown in Figure 59, Certify Vote. First, a bit by bit comparison is made of all memories. The Run Certification Recount Process, as shown in Figure 60, is also executed. It is this process which leads to a true election certification at the precinct level. As shown, two separate and distinct logical processes are employed to separately recount all the votes. The two separate logical processes are formed by two separate individuals who do not have contact with one

another. Each logical process may be realized through two separate computer programs. Due to inherently different styles between different computer programmers, each logical process will be separate and distinct. This procedure also provides an error checking function to ensure programming integrity, i.e., that a logical programming has not occurred.

Each logical process simply counts each vote of each voter record for each race. However, these separate processes have a different implementation of the logical processing necessary to recount the votes. A difference in the final tallies would immediately determine that a logical processing error existed. Each individual jurisdiction of use would specify what processing, actions, and/or methods would be performed for a failed precinct certification.

At completion of certification, if communications are present, the precinct certification data is sent to the next higher system element. This process also displays the vote results at the precinct. Establishing a processing method to detect logical processing errors and the incorporation of the on-line certification process are made part of this invention.

Figures 61, End Precinct, shows the "end precinct" process. This procedure locks out all inputs to the CPP and is used to bring the system to a known state prior to shut down.

On-Line Statistics

On-line statistics is another advance in this invention. The periodic processing performed by this procedure is shown in Figure 62, Statistics Processing Function. The data produced by the process is useful to both the public and election workers during the voting period and for election officials after the election. Statistics processed and available for display are:

A. At the precinct level
   1. Total number of precinct registered voters
   2. Total number of voters and by party
   3. Total number of ballot voting stations
   4. Voter throughput total, by each hour, and during last hour

5. Average time to vote and range
6. Number of help requests
7. Average help time and range
8. Number of poll workers
9. Total time poll open
10. Lost time due to problems
11. Number of security alerts
12. Election results

    In descending sequence by office, candidate's name, and number of votes

13. Wait time estimation
14. Precinct political division statistics including but not limited to:
    a. Legislative District
    b. Congressional District
    c. Council District
    d. Precinct District

B. At the city/county level

1. Same statistics as the precinct except totaled for entire city or county.
2. All of the above is displayed on a precinct by precinct basis
3. Operational status and number of voters by political division statistics including but not limited to:
    a. Legislative District
    b. Congressional District
    c. Council District
    d. Precinct District

C. At the State level

1. Same statistics as city county level except totaled for the entire state.
2. All of the above is displayed on a county by county or city-by-city basis.
3. Operational status and number of voters by political division statistics including but not limited to:

a. Legislative District
b. Congressional District
c. Council District
d. Precinct District

During the election, *voter throughput* and time to vote and other data can be released as public information to assist potential voters in deciding when to vote. The information could also be used by election officials to identify low voter throughput precincts and determine how throughput can be improved during the election. After the election, analysis of this data can be used to establish better methods of providing voter service.

Precinct System Displays

A specific set of operator displays are provided at the precinct for the purpose of operator interface and control. These displays are limited by the display structure as shown in Figure 16. Figure 19, System Start Up Screen, is the precinct start up display which shows each start up operation completed and provides for specific operator inputs. This methodology affords an additional degree of security by requiring an operational code entry. The operational code is provided by the system provider, and is sealed and shipped separately from the software.

Figure 23 is the precinct statistics display. The display of the statistical data on line is a significant feature of this invention. Figure 24 depicts the Help Status display.

City/County and State Level Systems and Processing

The hierarchical design of this invention allows the option of having a centralized city/county and/or state collection/control element as shown in Figure 1. The amount of centralized collection and control performed by the higher level system elements is specifically determined by the laws of the jurisdiction where the system is being used. The inclusion of the city/county and/or a state processor within this design provides the system's remote recording electronic (RRE)

capability. The following detailed description of the city/county/state level system describes a complete hierarchical control implementation in which any control function processing described could be excluded to accommodate jurisdiction laws or user requirements.

The specific purpose of the city/county and state system is to provide the functions necessary to allow centralized collection of votes in a real time secure manner and perform automated vote tallying at the city/county and/or state level. To perform this, functions are included for (1) secure communications, (2) data verification, (3) vote compilation, statistical data processing, (4) election certification, (5) public count and display, and (6) electronic data release.

As shown in Figure 3, the city/county system comprises the next higher collection and control element of the overall system above the precinct system. Some city/county systems will be further linked to the higher state level system as shown in Figure 1.

Figure 3 shows the components that comprise the city/county processing system. The city/county processor is a general purpose data processor. It is connected via a network controller or a functionally equivalent device to precincts, the state system if in use, and various public release subscribers through a one way data communications device.

The system provides for operator interface through the incorporation of a display, keyboard, and a set of specific data displays for the display structures as defined in Figures 16, 17 and 18. To facilitate the large numbers of persons who generally monitor the election from the city/county election offices, a provision has been made for a large screen projection display control station. The displays available are limited to data displays only. No control displays are available to the large screen projection display. Therefore, they are a subset of the displays of the city/county status display as shown in Figure 17.

Redundant data storage is provided through "n" memory systems. A mail-in vote entry station is provided for the entry

of absentee vote data. A physical key switch is also incorporated to allow security for supervisory level actions.

This hardware configuration is controlled by the logical processing functions of the city/county processor. The processing functions for the city/county processor include a pre-election test function, an operational election function, and post election processing functions.

Data communications between the city/county processor and the precincts are controlled by the city/county processor and a network controller or a functionally equivalent device. The network controller is electrically connected to a modem and a data encryption device. This configuration performs the encrypted data transfer over standard telephone lines as shown in Figure 1. Wireless, optical cable, and other data connections may also be used. Interface to the State level system, Figure 4, is afforded in the same manner.

Information generated by the city/county processor for public information release is transmitted to subscribers via a non-encrypted communications functional device. This line is a controlled one direction communication link for the city/county system to the subscriber. The system will only connect to subscribers it has called and it will not receive any data over these lines. The logical processing functions of the city/county processor continuously performs security processing to
monitor all exterior conditions.

An interface is provided for a mail-in ballot station. This interface allows mail-in votes to be integrated with the data collected from the precincts and automatically counted.

As shown in Figure 1, a maintenance/monitoring system is provided to allow the system provider to monitor the operating status of all systems in the election. The purpose is to allow for centralized support in the event of a failure at any level of the system. This allows for senior level decisions and failure procedures to be directed and monitored by supervisory level personnel.

City/County Processor Logical Processing Functions

Three general functions are performed by the city/county processor:

A. Pre-Election Stand Alone Test Function

B. Operational Election Function

C. Post Election Processing Function

Control functions performed by the city/county and state processors, as shown in Figure 63, include (1) time synchronization, (2) communications control, (3) vote authorization, (4) poll opening, (5) poll closing, (6) election certification, (7) election status display, (8) poll restart commands, and (9) maintenance commands. These control functions are changed for each jurisdiction to accommodate local laws and community desires and may be entirely eliminated.

Pre-Election Stand-Alone Test Function

The purpose of the pre-election stand-alone test function is to test and verify the complete operation of the entire RRE system prior to the conduct of the election as shown in Figure 64. Processing performed by this function emulates all processes to be performed during the actual election and includes all communications, data verification, data collection and operator processing. The city/county processor collects and records the stand alone precinct test results, their audit trails, and creates and records its own audit trail. These records will form a critical part of the evidence required to validate the system's operation if any challenges should be made to an election result generated by the system. The pre-election test function command set and the data created and processed during the pre-election test are impounded and archived after the test.

Detailed Description of the City/County Pre-Election Test Function

Figure 64, Pre-Election Test Function, depicts the overall pre-election test processing at the city/county level. The first process performed is the self-validation process as shown

in Figure 15. If this test passes, then the data storage areas are validated and zeroed to assure that no failed memory locations are present in the data storage area as shown in Figure 65, Verify Storage & Set Precinct VO.

As shown in Figure 66, Set Up Precincts & VO Channels, communication preprocessing is performed to set up input channels to communicate with valid precincts. Communications processing waits for communications to begin when each precinct calls. When the precinct communications are established, the transmitted security code from the precinct is validated. The system then hangs up at that point and builds a call back schedule. This processing is depicted in Figure 67, Process Secure Communications. This processing is started by an initial precinct call in.

Once a precinct has been validated, open communication processing recalls the precinct and establishes communications as shown in Figure 68, Open Communications.

Data input to the city/county processor from the precincts is validated and stored in redundant memories as shown in Figure 69, Collect Pre-Test Data. Input data is validated by verifying the precinct data checksum.

If this test passes, the data is stored in redundant memory locations. If a failure occurs, then the input/output fault process is scheduled to run.

Pre-test certification is run at the end of the pre-test after all data has been collected as shown in Figure 70, Certify Pre-Test. This process validates that the data received from each precinct agrees with a test script. Certification is good if the received data is in agreement with the scripted data expected.

In the event of a failed certification, a certification failed process is performed. The specific processing performed by this process is implemented specifically as required by the desires and laws of the jurisdiction of use.

The shut down pre-test process closes all in/out channels and brings the system to known quiescence so that power can be turned off. Once this is done all memory media from the system

components is removed, sealed and impounded as shown in Figure 5.

Operational Election Logical Processing Function

The Operational Election Logical Processing Function is used for the conduct of the official election and is shown in Figure 72. After Self-Validation, secure communications processing is performed to establish communication with its connected precincts.

When the communications link to the precincts is established, the validate precinct processing shown in Figure 73 is performed.

Once the precinct connection is established and confirmed, an election pre-test is performed to validate the operation of the RRE system with the operational election software. This pre-election test is a statistically significant subset of the stand alone pre-election test previously described. The results of this test are also certified as described in the stand alone test processing. This process is illustrated in Figure 72. If the Pre-Election Test is successful, the polls are opened as shown on Figure 71, Open Polls Command.

Figure 73, Run Secure Communications, shows the processing performed by the secure communications procedure of the city/county processor. The first function performed is the set up of a randomly generated hang-up call-back process as shown in this Figure. This processing determines (1) when the next call to a precinct will be made, (2) whether the call will be initiated by the precinct or the city/county processor and (3) the duration between calls. Security processing is initiated if the time between calls is exceeded or if a connection can not be established.

Once the communication link is established, a series of security codes are exchanged validating that both the correct connection has been established and that no line tampering and/or tapping has occurred. During this time, the precinct software is checked for tampering. Again any failure detected would invoke special security processing that would alert the

system operators and trace the suspected security breach.

The next process performed by the secure communication procedure is to validate the precinct and confirm its processing status. If the precinct is valid and the precinct is in voting status, a secure communications routine sets up a read vote data command.

These read vote commands are based on the end time of the last communication minus five minutes to current time. The duplication of retransmitting the data already stored from the last read is a double check of the data being received. See Figure 74, Validate Precinct.

The next procedure performed collects and verifies the vote data. The collect vote data procedure is shown in Figure 75, Collect Vote Data. The procedure reads the data from the time of last call minus "X" minutes to current time. The data is then retransmitted back to the precinct and verified. If the data is good, the process stores the valid election data. If it is not good, the process will retry three (3) times before activating security processing to determine the cause of the failure.

A feature of this invention is the centralized on-line certification capability. The processing required to perform this procedure is shown in Figure 76, Certify Election.

Once the precinct goes to poll closed status, the precinct processor performs the precinct level certification. At the conclusion of this process, the precinct sends a status of "certification done" to the city/county processor. If the precinct certification is good, the certify election procedure reads in a complete set of vote data and the audit log. A bit-by-bit comparison of the certified precinct data and the data compiled over the course of the election at the city/county level is then made and the entire vote is recounted and compared with the certified precinct tallies. If the status of these comparisons is good, the certification procedure establishes the good election status and displays certification complete. The certification processing is a critical part of this invention. The specifically defined voter record and critical data

processing methods of the present invention enable the foregoing process. Local election officials will specify the processing and/or procedures to be performed if on-line certification fails. This will be implemented on a per election, per location basis.

These voter records are used by several different logical vote counting processes which will eliminate the possibility of logical processing errors or mistakes which would provide an erroneous election result. The display election procedure shown in Figure 77, Display Election Returns, is then processed to display the election results. The controlling official at the city/county level can then, if desired, release the election results electronically to any connected subscribers. If certain races cannot be certified, the release would indicate "preliminary results-count with 'X' precincts certified". The final process performed by the city/county processor is the "shut down" process depicted in Figure 78, Shutdown Election.

City/County Displays

The city/county displays are similar to the precinct level displays. Figure 25, City/County Status Display, shows the status of the entire city/county system. Figure 26, City/County Statistics Display, shows the county statistics. This selection can include city/county political divisions such as council districts, congressional districts, and others.

Figure 27, Select Precinct Display, allows the operator to select individual precinct data for display. The operator can select either the precinct status or statistics display.

City/County Off-Line Data Processing Function

The purpose of this function is to provide for access and analysis of the election records saved during the election. Figure 10 shows the functions performed by the off-line post election computer program. The system necessary for this processing is shown in Figure 3. The functions required for post processing will vary from county to county; however, the basic functions provided are:

1.) Review precinct "X" voter records
2.) Review precinct "X" audit trail
3.) Compile statistics
4.) Print data
5.) Review mail-in voter records
6.) Recount race
7.) Review time sequence
8.) Display test data

State Level System

Figure 4 shows the optional state level system of the RRE system. This system configuration and its logical processing functions are the same as those described for the city/county system except that the state system inputs are from connected city/county systems and that the election display and tally functions cover the entire state.

I claim:

1. A recordable voting system audit trail detailing a plurality of voting system events which occur at a plurality of corresponding times in a time ordered sequence comprising:

record unique data including voting system event information corresponding to a voting system event of said plurality of voting system events; and

a time tag indicating a time corresponding to when the voting system event occurred.

2. The recordable voting system audit trail according to claim 1, further comprising:

a recordable medium which records the record unique data and the corresponding time tag;

a log entry time corresponding to the time that the record unique data and time tag are stored in the recordable medium.

3. The recordable voting system audit trail according to claim 1, further comprising:

a plurality of record unique data including a corresponding plurality of voting system event information, each detailing a voting system event; and

a plurality of time tags indicating a plurality of corresponding times when said voting system events occurred.

4. The recordable voting system audit trail according to claim 3, further comprising:

a recordable medium which records said record unique data and said corresponding time tags;

a plurality of log entry times corresponding to the times that the critical data elements and time tag are stored in the recordable medium.

5. The recordable voting system audit trail according to claim 1, wherein said time tag is comprised of a plurality of digital information bits and said audit trail includes a critical data element which includes said time tag, said audit trail

comprising:

a critical data element header having a number of digital information bits corresponding to a predetermined data type of a plurality of data types and a predetermined number of digital information bits indicating said time tag; and

a header checksum which indicates a number of data bits in the critical data element header.

6. The recordable voting system audit trail according to claim 1, wherein said time tag is comprised of a plurality of digital information bits, said critical data element comprising:

a data checksum which indicates a number of data bits in the record unique data.

7. The recordable voting system audit trail according to claim 1, wherein said time tag is comprised of a plurality of digital information bits, and said audit trail includes a critical data element which includes said time tag, said audit trail comprising:

a critical data element header having a number of digital information bits corresponding to a predetermined data type of a plurality of data types and a predetermined number of digital information bits indicating said time tag; and

a header checksum which indicates a number of data bits in the critical data element header; and

a data checksum which indicates a number of data bits in the record unique data.

8. The recordable voting system audit trail according to claim 7 further comprising:

a critical data element checksum which indicates a number of data bits in the critical data element.

9. A voting system individual voter record detailing voter information corresponding to a vote cast by a voter, said individual voter record comprising:

a critical data element header including a time tag

indicating a time corresponding to when the voting system event occurred; and

voting system event information corresponding to a voting system event of said plurality of voting system events.

10. The voting system individual voter record according to claim 9, wherein a voter key card includes voter key card identification information, said individual voter record further comprising:

a voter key card identification corresponding to said voter key card identification information.

11. The voting system individual voter record according to claim 9, wherein a voter enters a vote into a voting system, said individual voter record further comprising:

ballot data indicating the vote selected by the voter in the voting system.

12. The voting system individual voter record according to claim 9, wherein a voter enters vote information into a voting system including a plurality of electronic ballots, said individual voter record further comprising:

a start time indicating a time when the voter initiated entry of the vote information into the voting system;

an end time indicating a time when the voter ended entry of the vote information into the voting system;

an electronic ballot number corresponding to a predetermined electronic ballot of said plurality of electronic ballots; and

a ballot checksum indicating a number corresponding to the start time, end time and electronic ballot number.

13. The voting system individual voter record according to claim 12, further comprising:

elapsed time information corresponding to a difference between said start time and said end time;

14. 12. The voting system individual voter record according to claim 9 wherein the critical data element header has a number of digital information bits corresponding to a predetermined data type of a plurality of data types and a predetermined number of digital information bits indicating said time tag, said individual voter record further comprising:

a header checksum which indicates a number of data bits in the critical data element header.

15. A remote recording computer voting system comprising:

a precinct system comprising a plurality of individual voter ballots, wherein each individual voter ballot receives a corresponding plurality of voter information;

a remote centralized vote collection station in a remote geographical location from said precinct system and in electrical communication with said precinct system which receives said plurality of voter information from said precinct system.

16. The remote recording computer voting system according to claim 15, wherein each of the plurality of individual voter ballots is a disposable voter ballot, said voting system further comprising:

a precinct processor disposed within the precinct system which communicates with the plurality of voter ballots to receive voter information therefrom; and

a nonvolatile memory connected to the precinct processor for storing the voter information received from the precinct processor.

17. The remote recording computer voting system according to claim 16 wherein the precinct processor provides a centralized start and central stop command to each of the plurality of voter ballots, said precinct processor providing encrypted data transmission between with each of the voter ballots.

18. The remote recording computer voting system according to

claim 15 further comprising:

a second precinct system comprising a plurality of second individual voter ballots, wherein each of said second individual voter ballots receives a corresponding plurality of second voter information;

wherein the remote centralized vote collection station is in electrical communication with said second precinct system and receiving said second plurality of voter information from said second precinct system.

19. The remote recording computer voting system according to claim 15 further comprising:

a first modem encrypter electrically connected to the precinct system for encrypting said voter information;

a second modem encrypter electrically connected to the remote centralized vote collection station and in electrical communication with said first modem receiving said voter information from said precinct system.

20. A method of electronically producing a voting event record for a voting event comprising the steps of:

electronically recording a voting event time;

electronically recording a voting event category representing a category of a voting event; and

electronically recording event data corresponding to the voting event.

21. The method according to claim 20 wherein the voting event is one of a plurality of voting events, said method comprising the step of recording each of the plurality of voting events in a time ordered sequence.

22. The method according to claim 20 said method further comprising the step of producing word parity information for each word of the saved data.

23. The method according to claim 20 said method further

comprising the steps of:

producing a data type unique header to specifically identify the voting event record; and

formulating an event data checksum representing a number of electronic data bits required to store the event data.

24. The method according to claim 20, wherein said method further comprises the step of:

formulating a header data checksum representing a number of electronic data bits required to store the data type unique header, the voting event category, and the header checksum itself.

25. The method according to claim 20, wherein said method further comprises the steps of:

producing a data type unique header to specifically identify the voting event record;

formulating an event data checksum representing a number of electronic data bits required to store the event data;

formulating a header data checksum representing a number of electronic data bits required to store the data type unique header, the voting event category, and the header checksum itself; and

formulating a total data checksum representing a number of electronic data bits required to store the voting event time, voting event category, event data corresponding to the data event, the data type unique header, the event data checksum, the header data checksum, and the total data checksum.

26. The method according to claim 25, wherein said voting event category, event data corresponding to the data event, the data type unique header, the event data checksum, the header data checksum, and the total data checksum all form a critical data element, said method further comprising the step of storing the critical data element.

27. The method according to claim 25 further comprising the

step of electronically recording a log entry time.

RRE= Remote Recording Electronic

* Encrypted Data Communication Lines

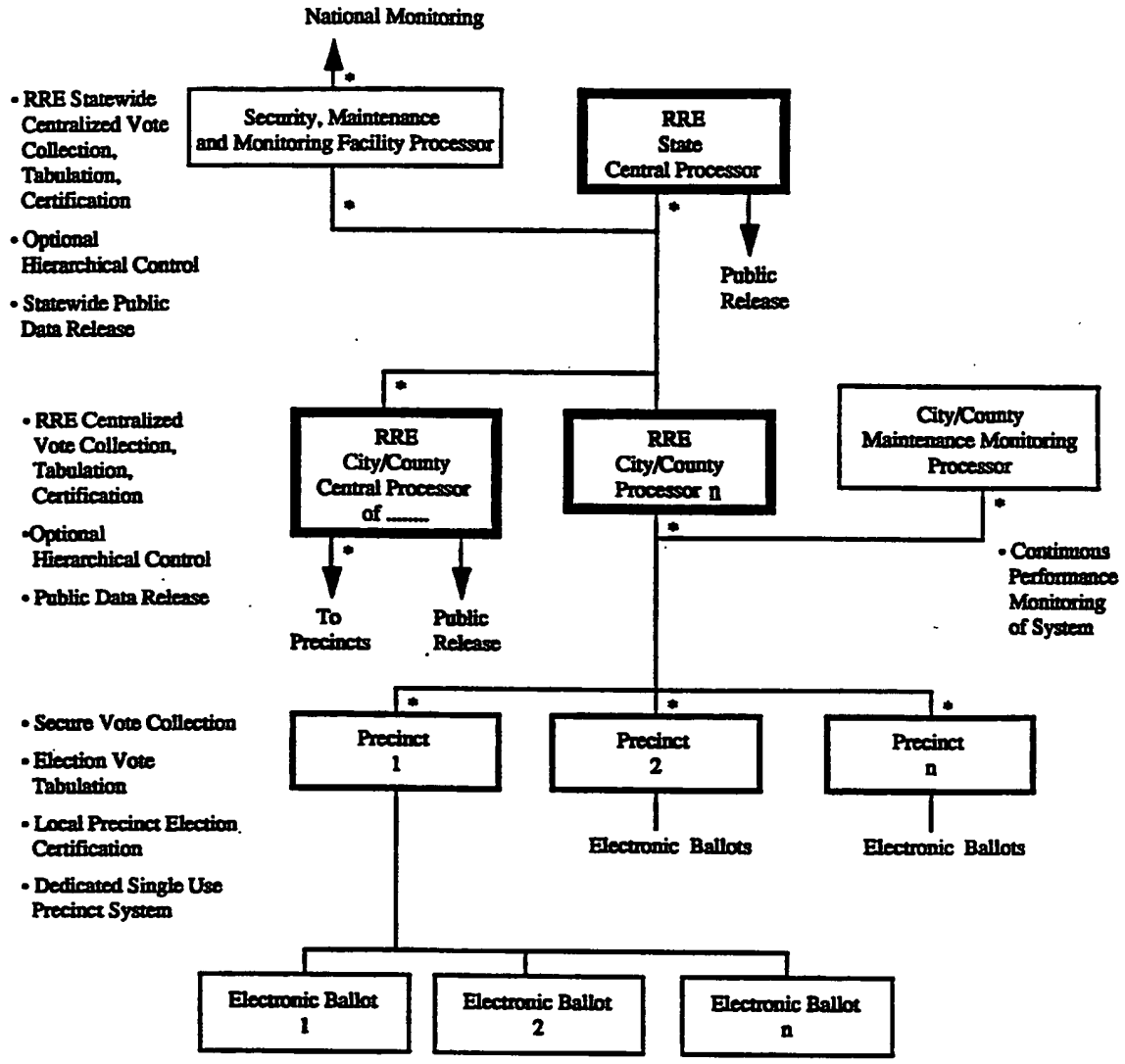


FIGURE 1 • Voting System Block Diagram & Functional Allocation

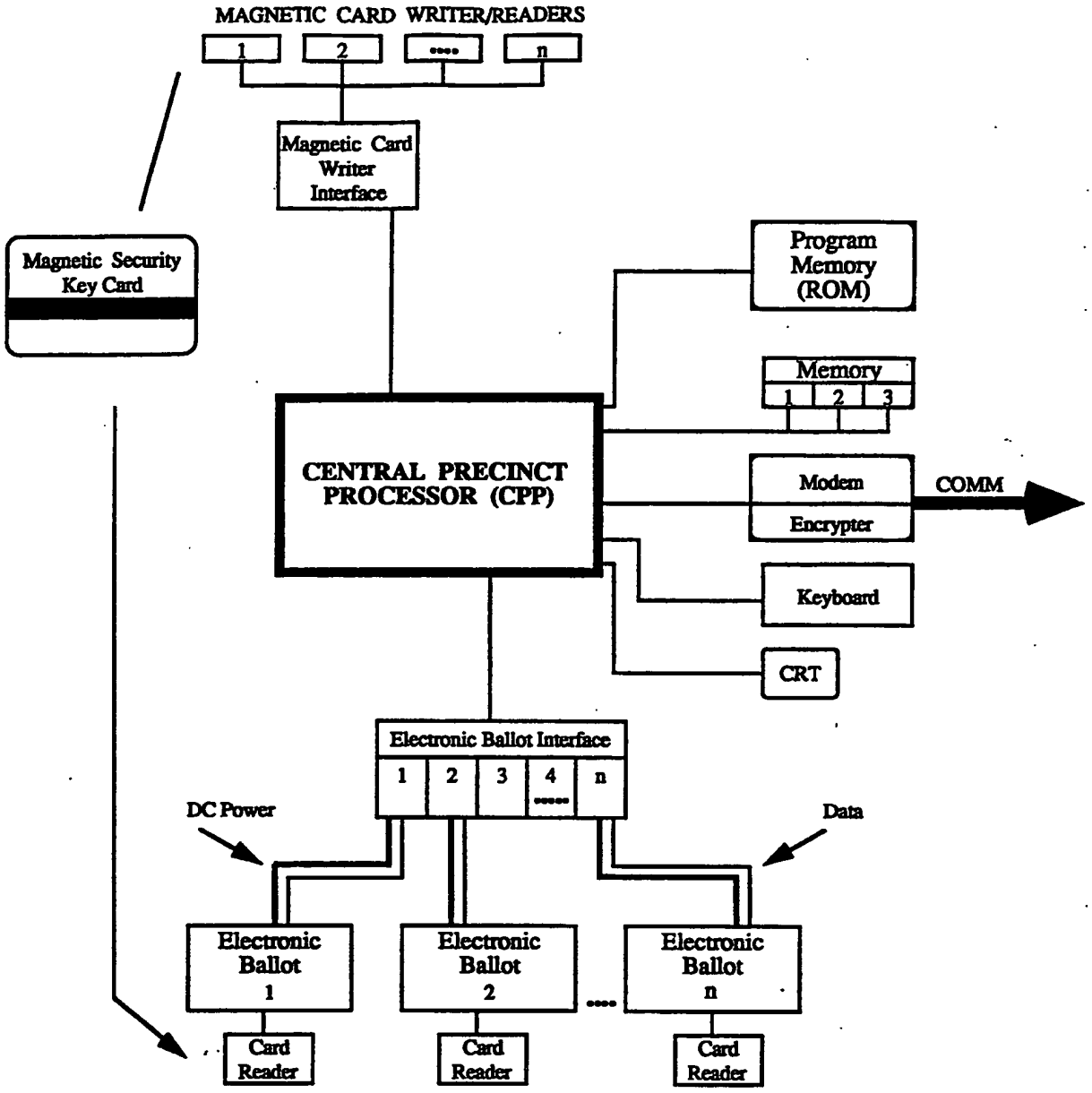


FIGURE 2 • Precinct System Diagram

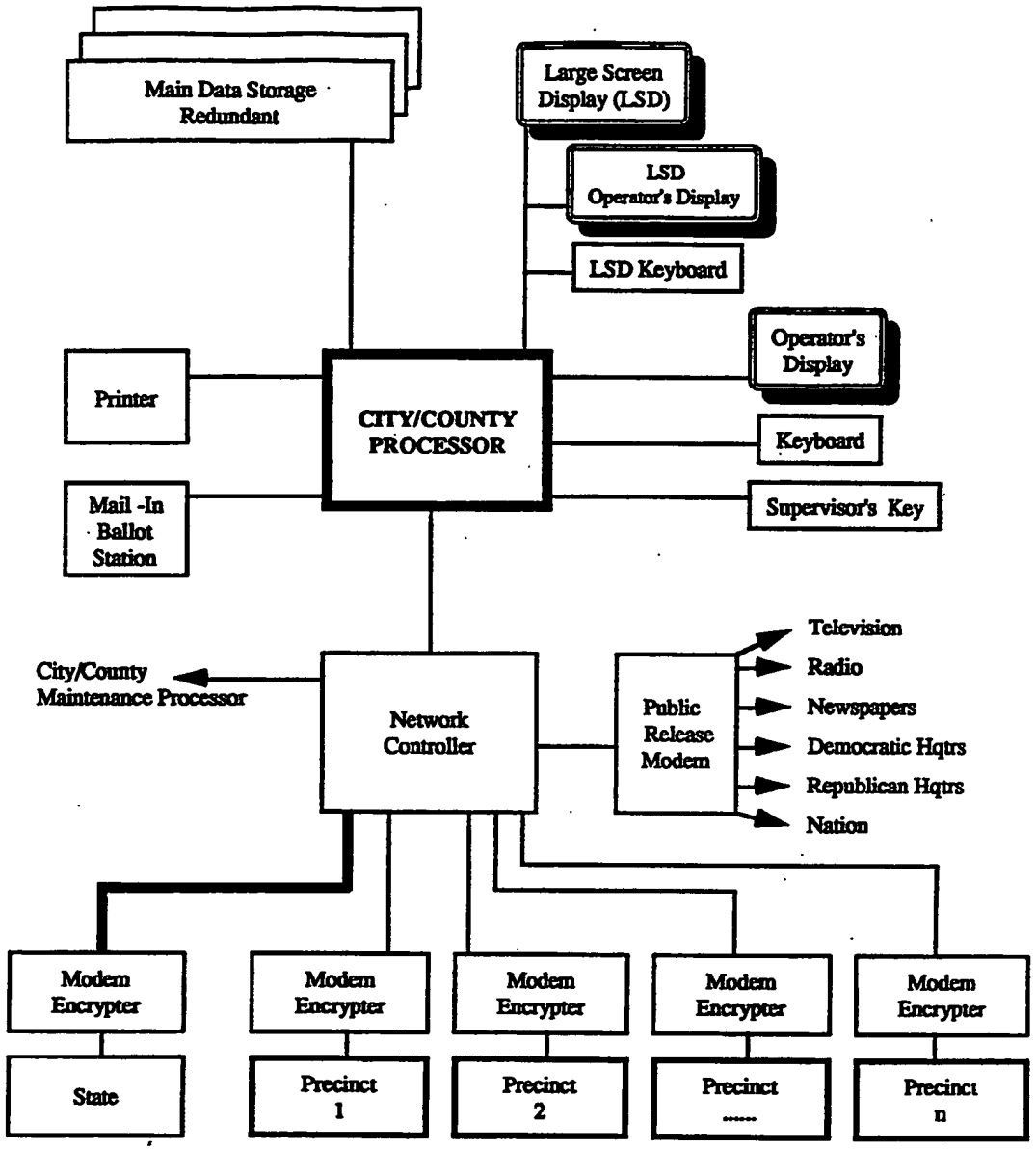


FIGURE 3 • City/County Block Diagram,
Remote Recording Electronic (RRE) Configuration

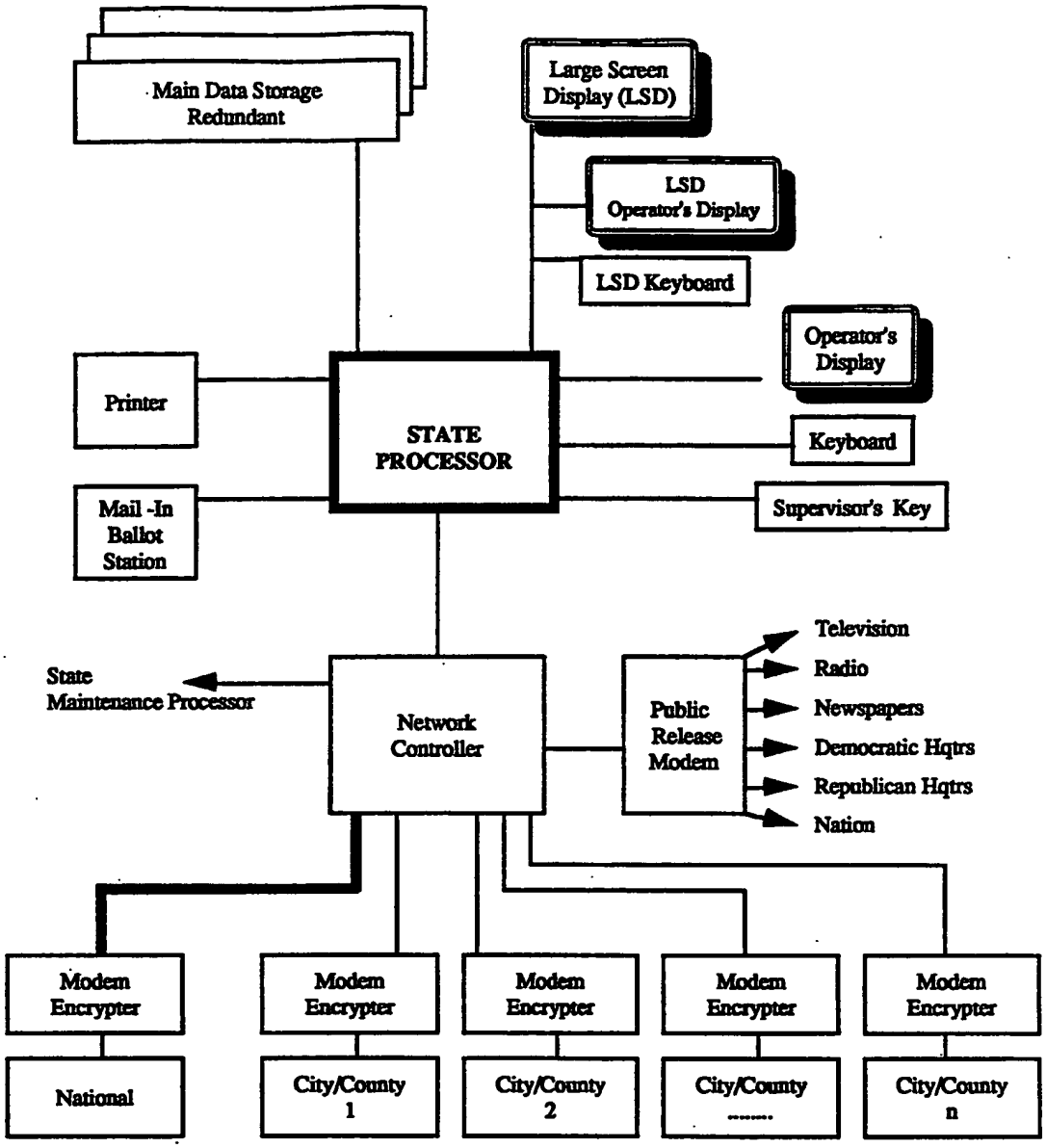


FIGURE 4 • State Block Diagram
Remote Recording Electronic (RRE) Configuration

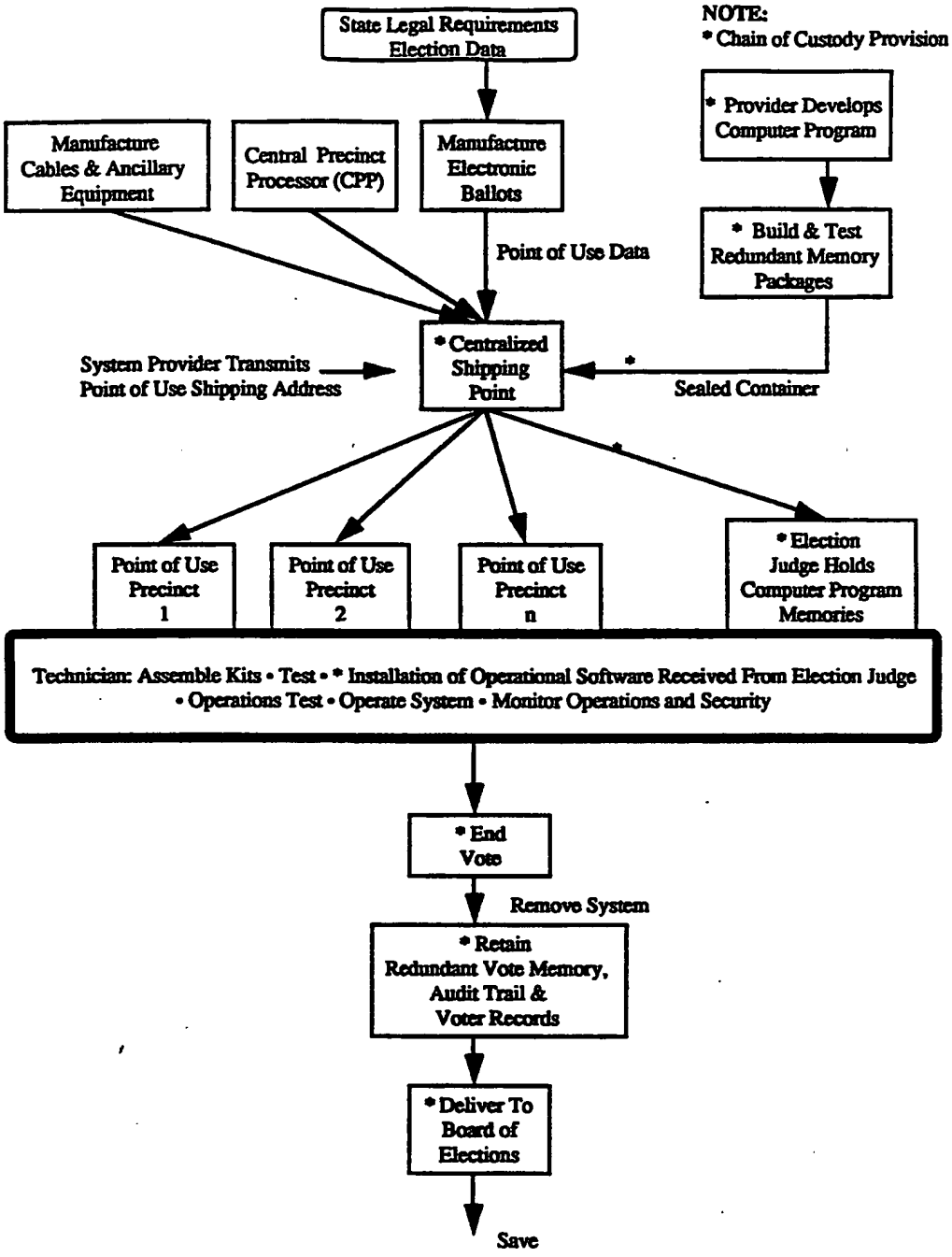
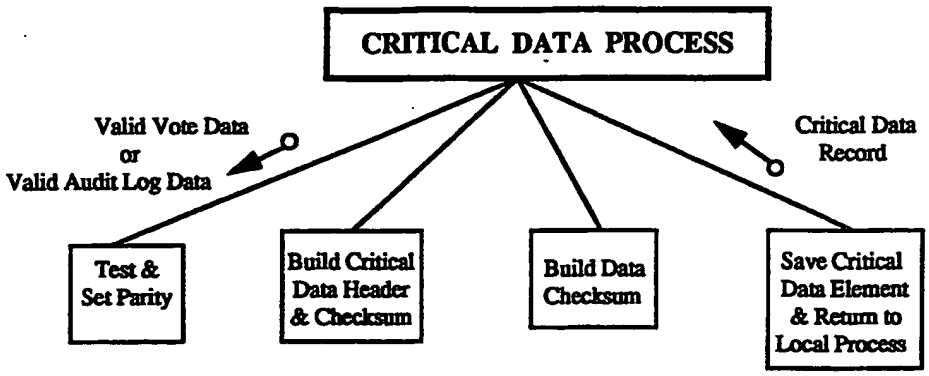


FIGURE 5 • Secure Single-Use Voting System Method



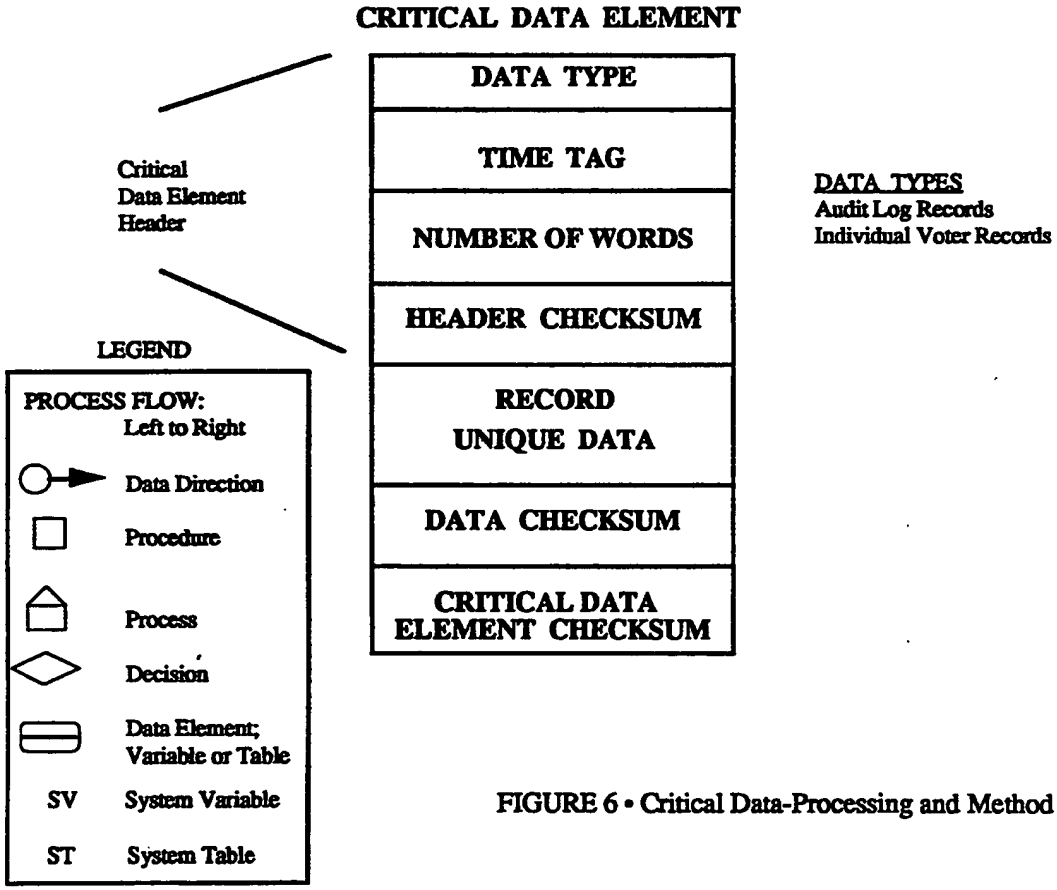
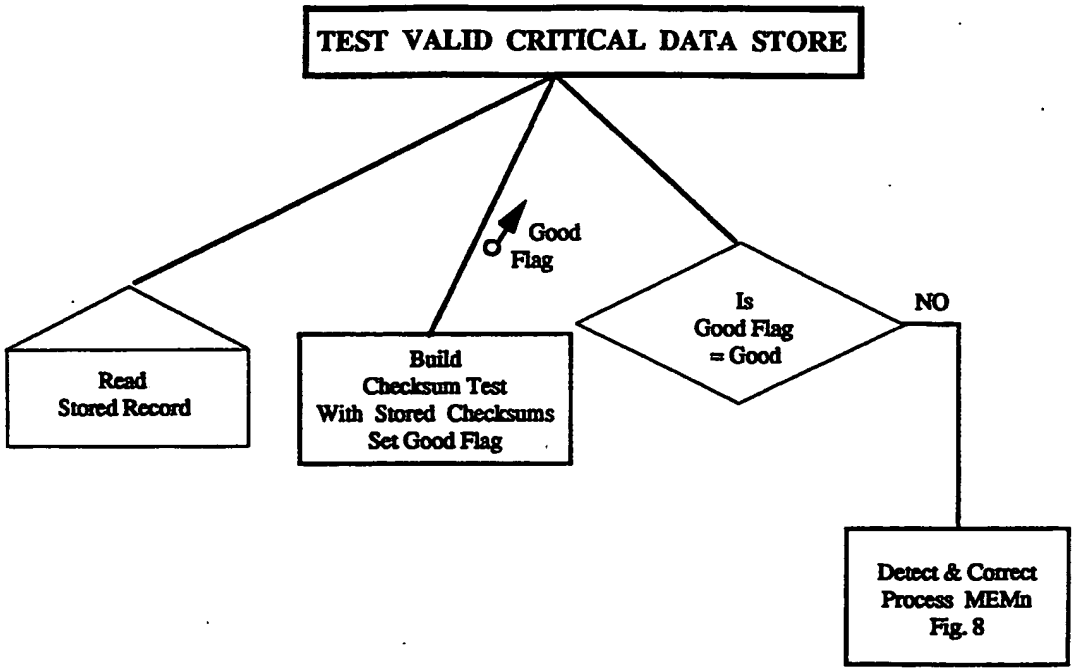


FIGURE 6 • Critical Data-Processing and Method



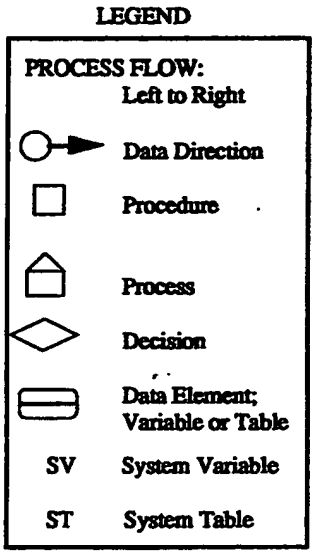
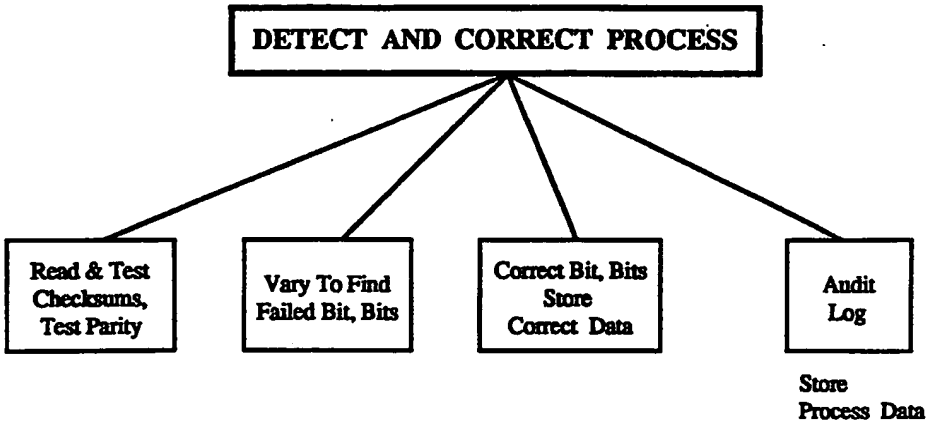


FIGURE 7 • Test Valid Critical Data Store Method



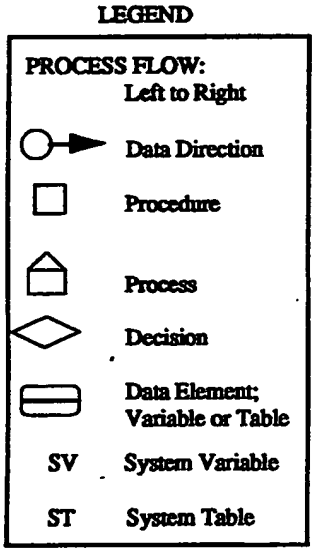
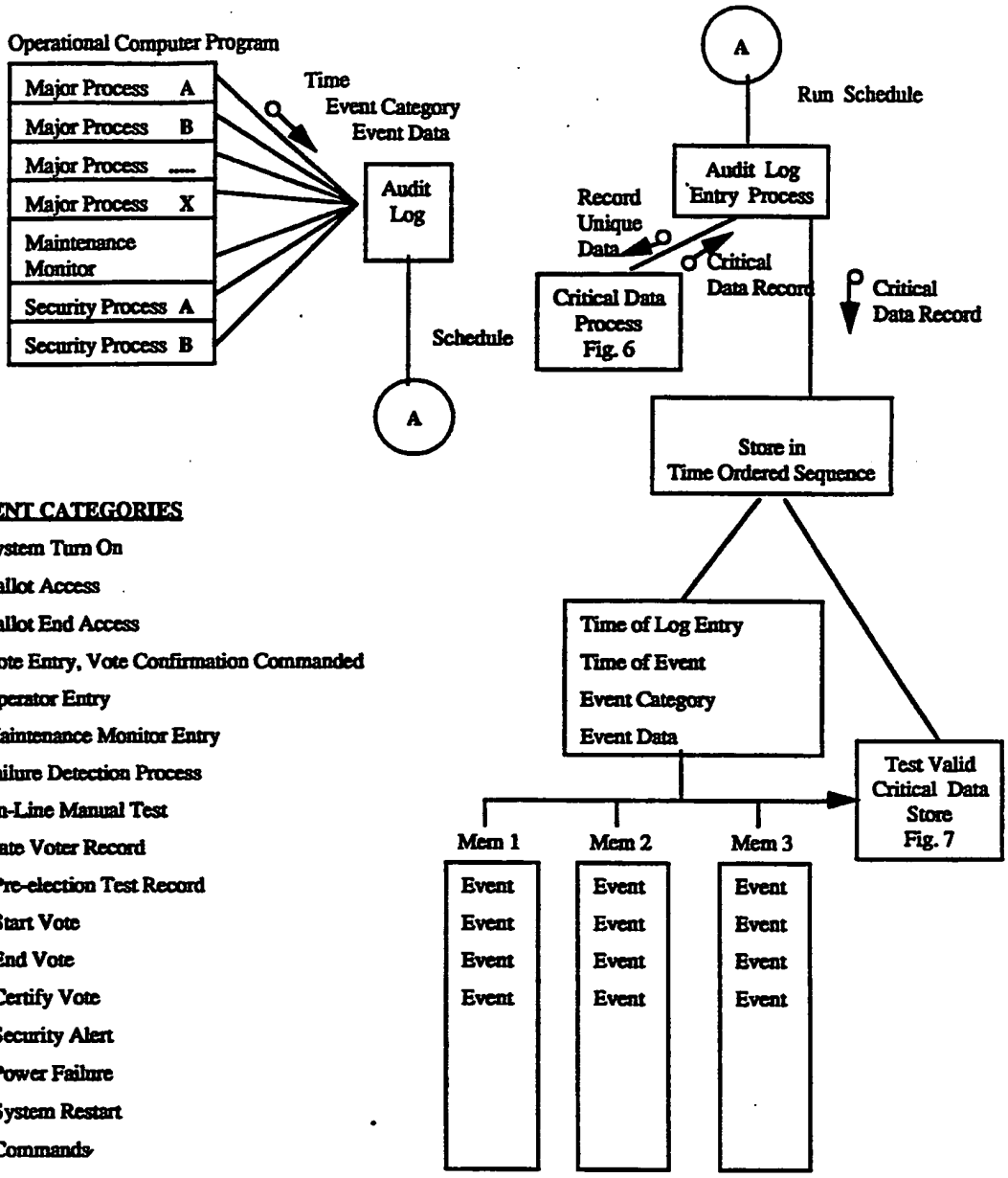


FIGURE 8 • Detect and Correct Process Method



EVENT CATEGORIES

1. System Turn On
2. Ballot Access
3. Ballot End Access
4. Vote Entry, Vote Confirmation Commanded
5. Operator Entry
6. Maintenance Monitor Entry
7. Failure Detection Process
8. On-Line Manual Test
9. State Voter Record
10. Pre-election Test Record
11. Start Vote
12. End Vote
13. Certify Vote
14. Security Alert
15. Power Failure
16. System Restart
17. Commands
18. Communication Processes
19. Voter Help Processes
20. System Shut Down Command

FIGURE 9 • Audit Trail Processing Functional Block Diagram

TIME	EVENT	PROCESS ACTION
10:00:00	Vote Entry	Ballot 10 Switch 2,4
10:00:01	Maintenance Monitor	Ballot 1 I/O tested OK
10:00:02	Maintenance Monitor	Ballot 2 " " "
10:00:03	Operator Entry	Write Key Card # 10000352
10:00:04	Maintenance Monitor	Ballot 3 I/O tested OK
10:00:05	Vote Entry	Ballot 2 Switch 10,3
10:00:06	Communication Process	City Read Command Send Data
10:00:07	Communication Process	City I/O Ack Sent Data 10:00 to 10:00
10:00:08	End Vote	Ballot 5 End Vote Commanded
10:00:09	End Vote Process	Stored Valid Voter Record
10:00:10	End Vote Process	Reset Ballot 5

FIGURE 9A • Audit Log Post Election Processing Verification Report

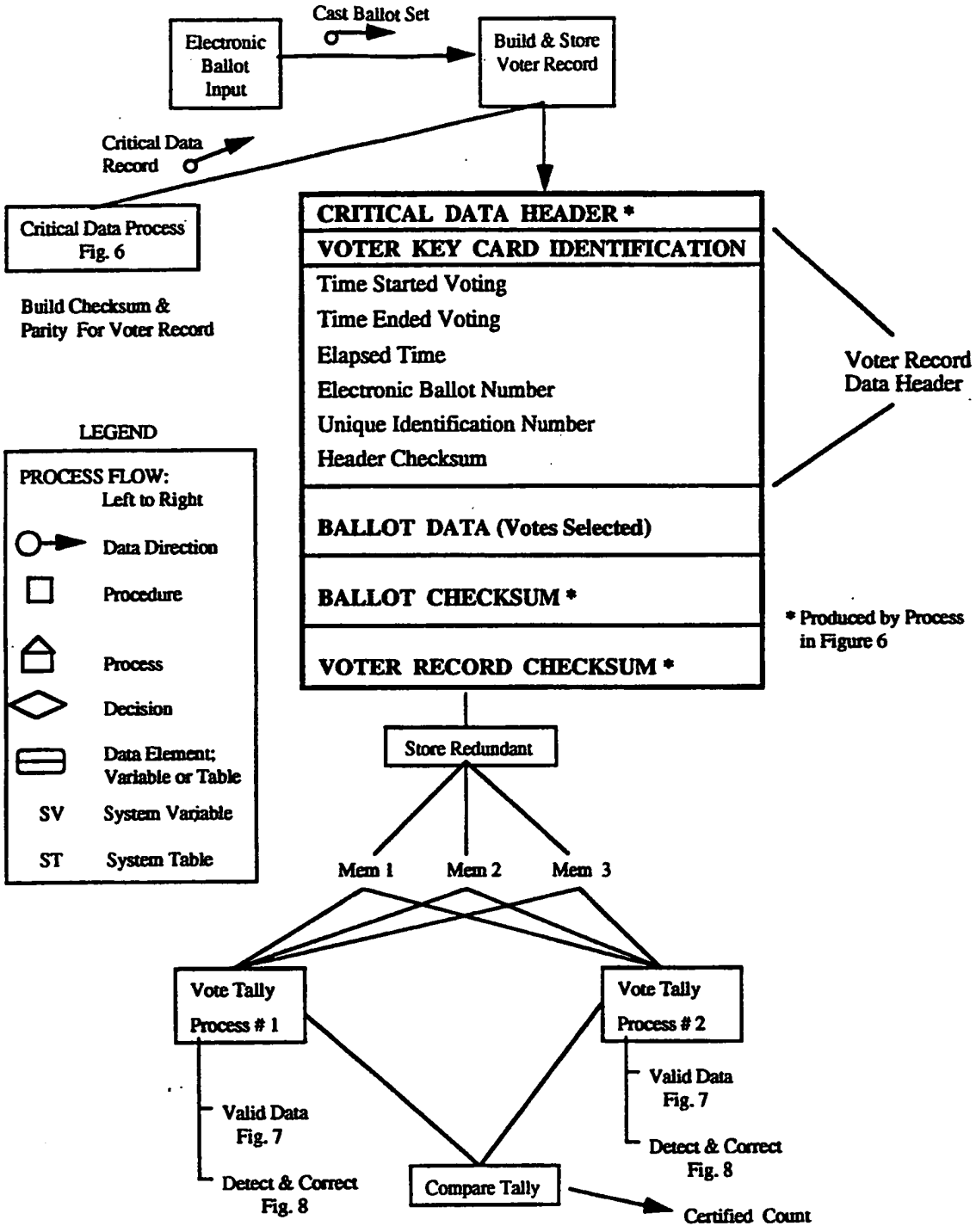


FIGURE 10 • Electronic Voter Record and Vote Tally Processing Functions and Method

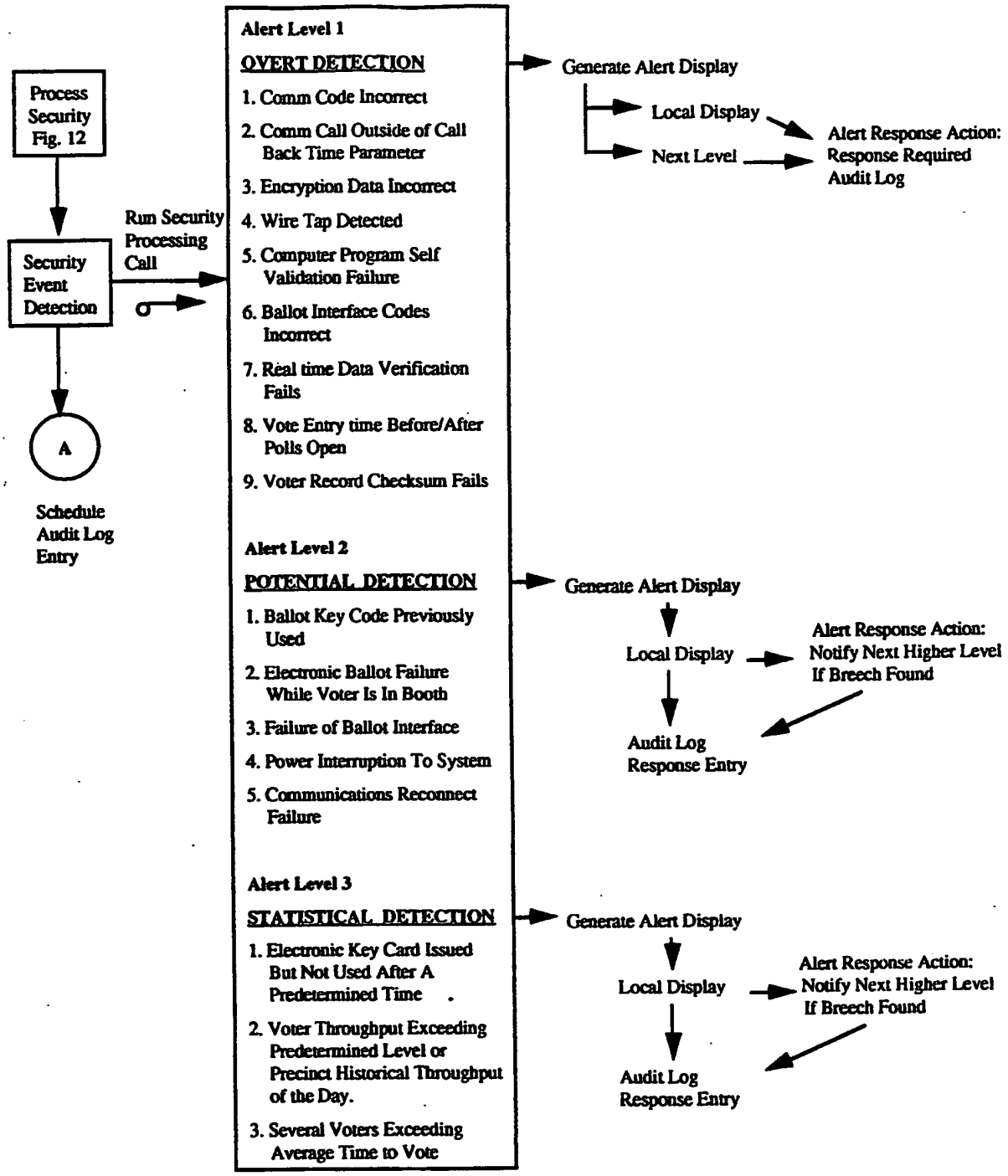


FIGURE 11 • Security Processing Functional Block Diagram

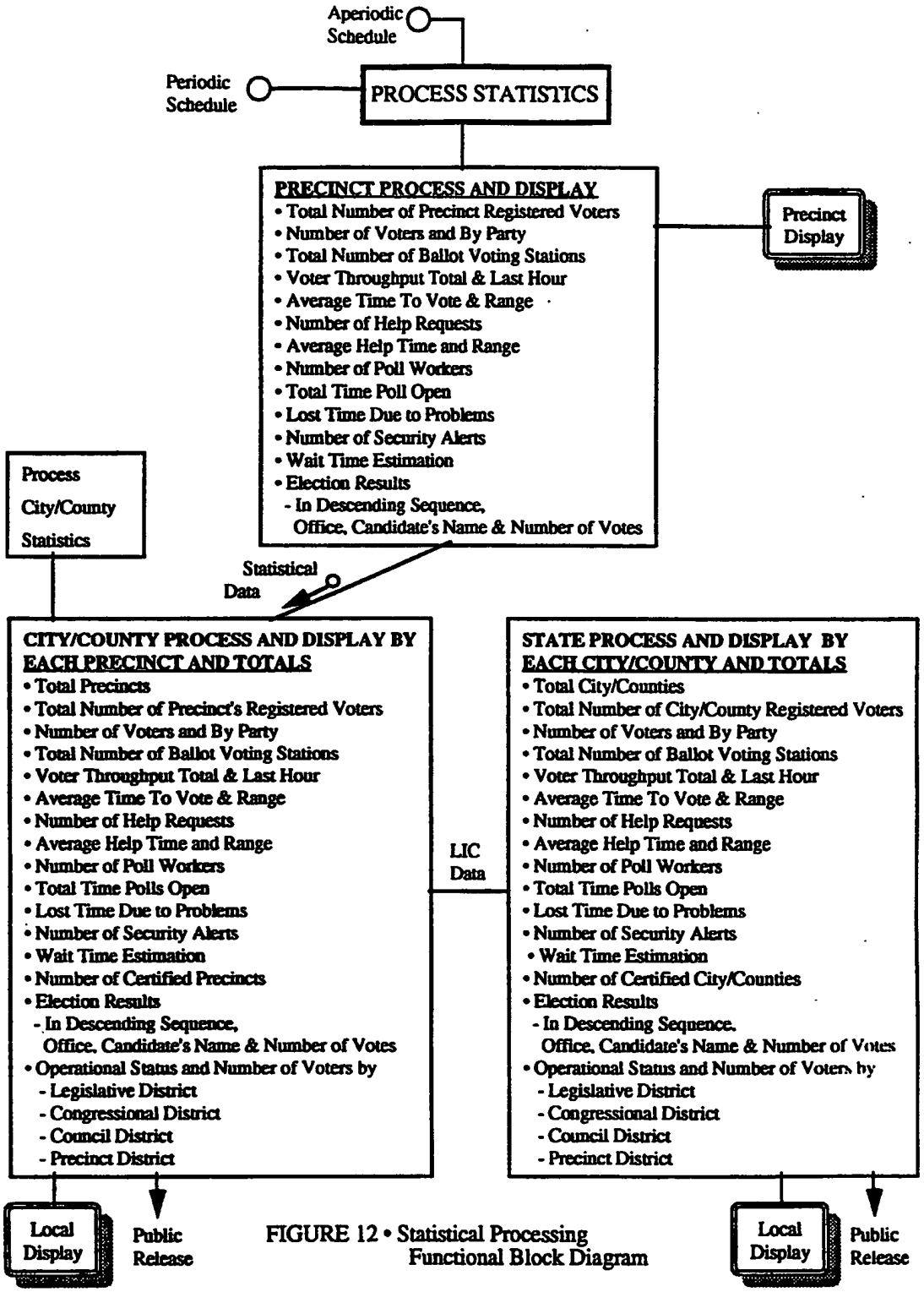


FIGURE 12 • Statistical Processing Functional Block Diagram

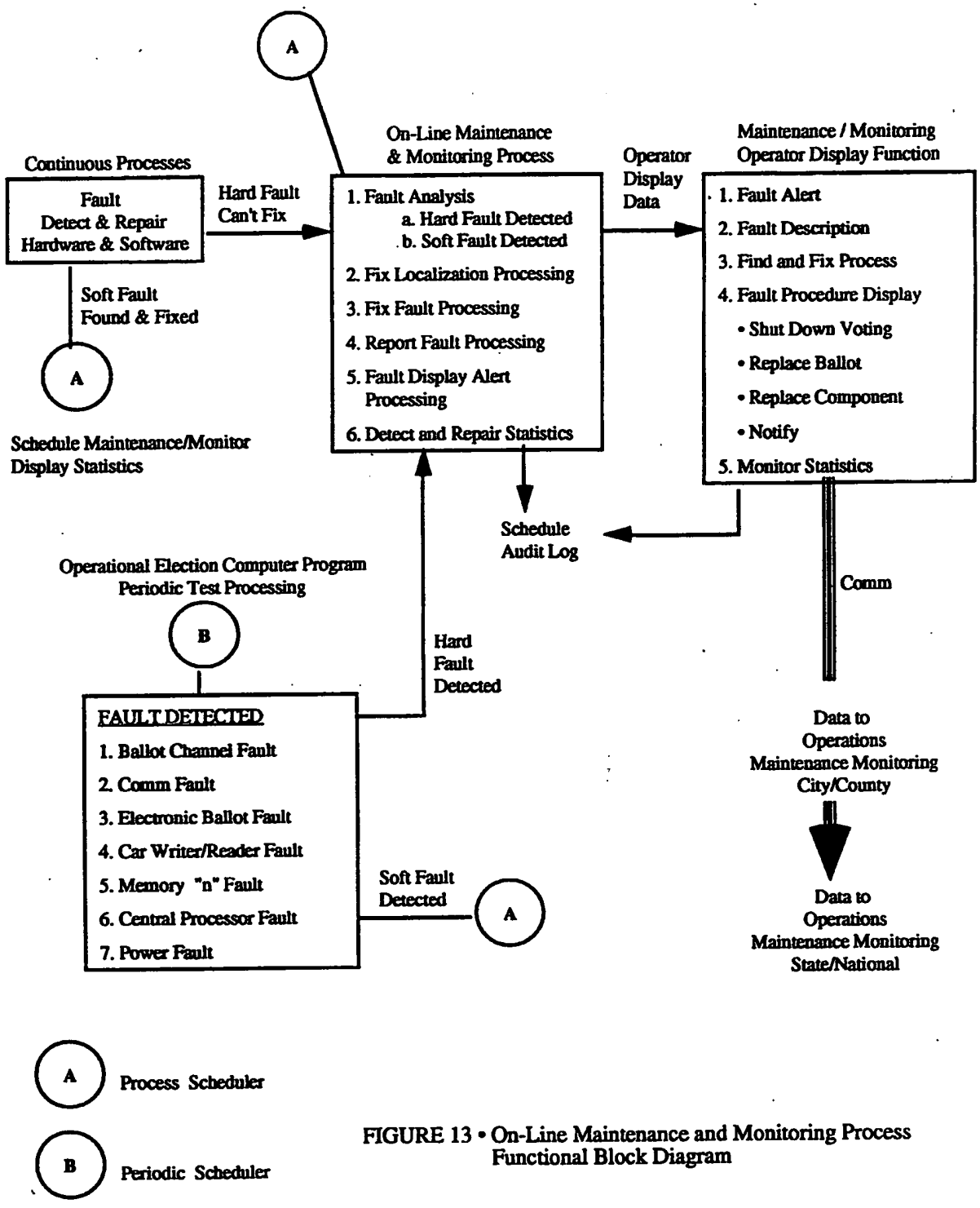


FIGURE 13 • On-Line Maintenance and Monitoring Process Functional Block Diagram

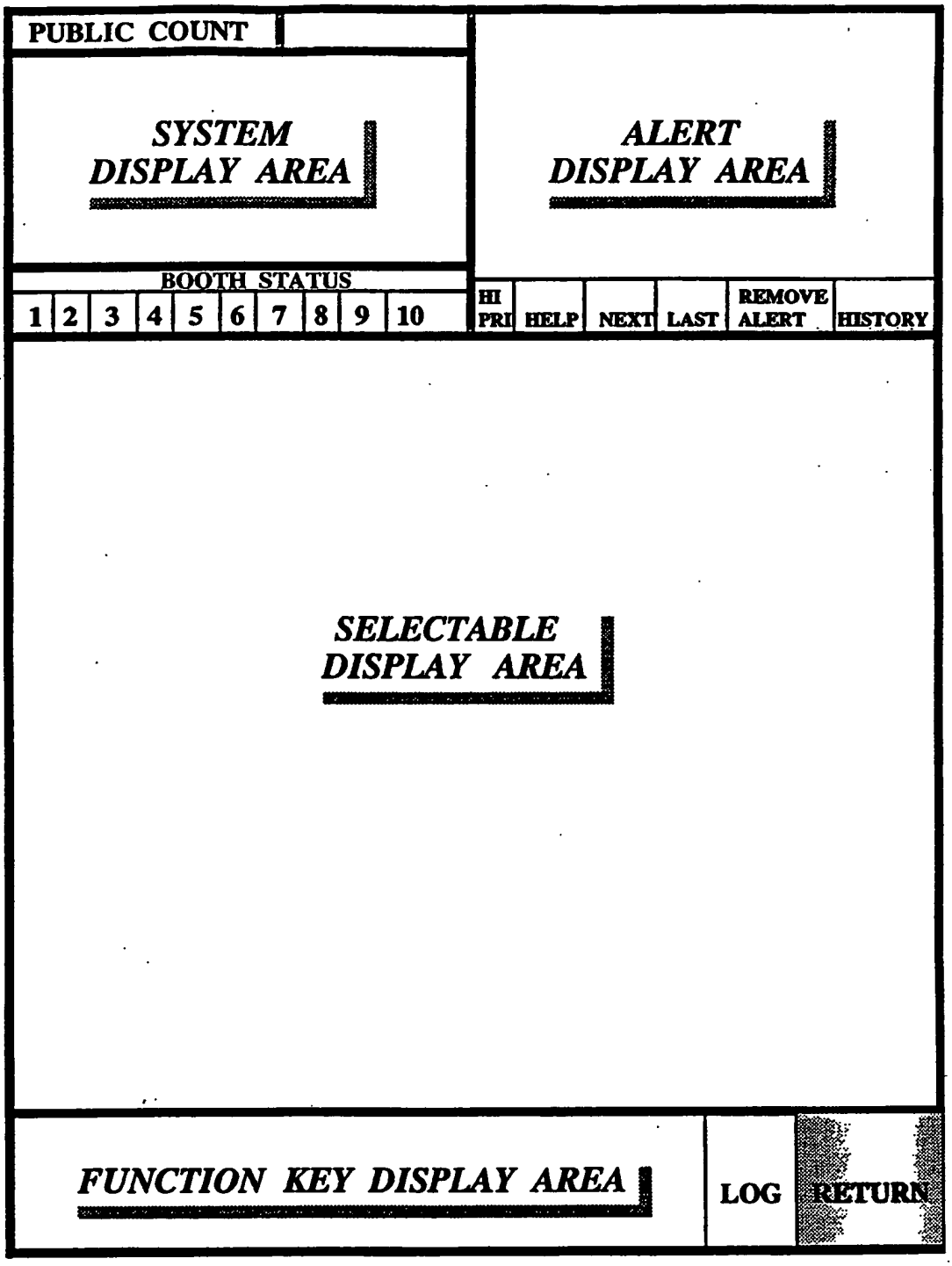


FIGURE 14 • Display Format

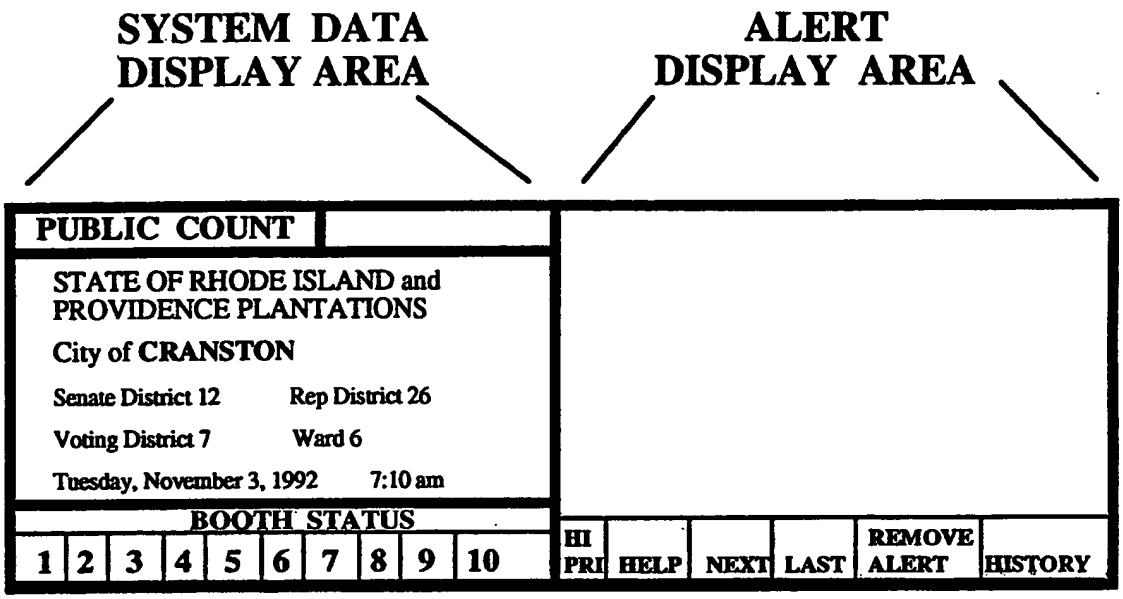


FIGURE 15 • Typical System Display

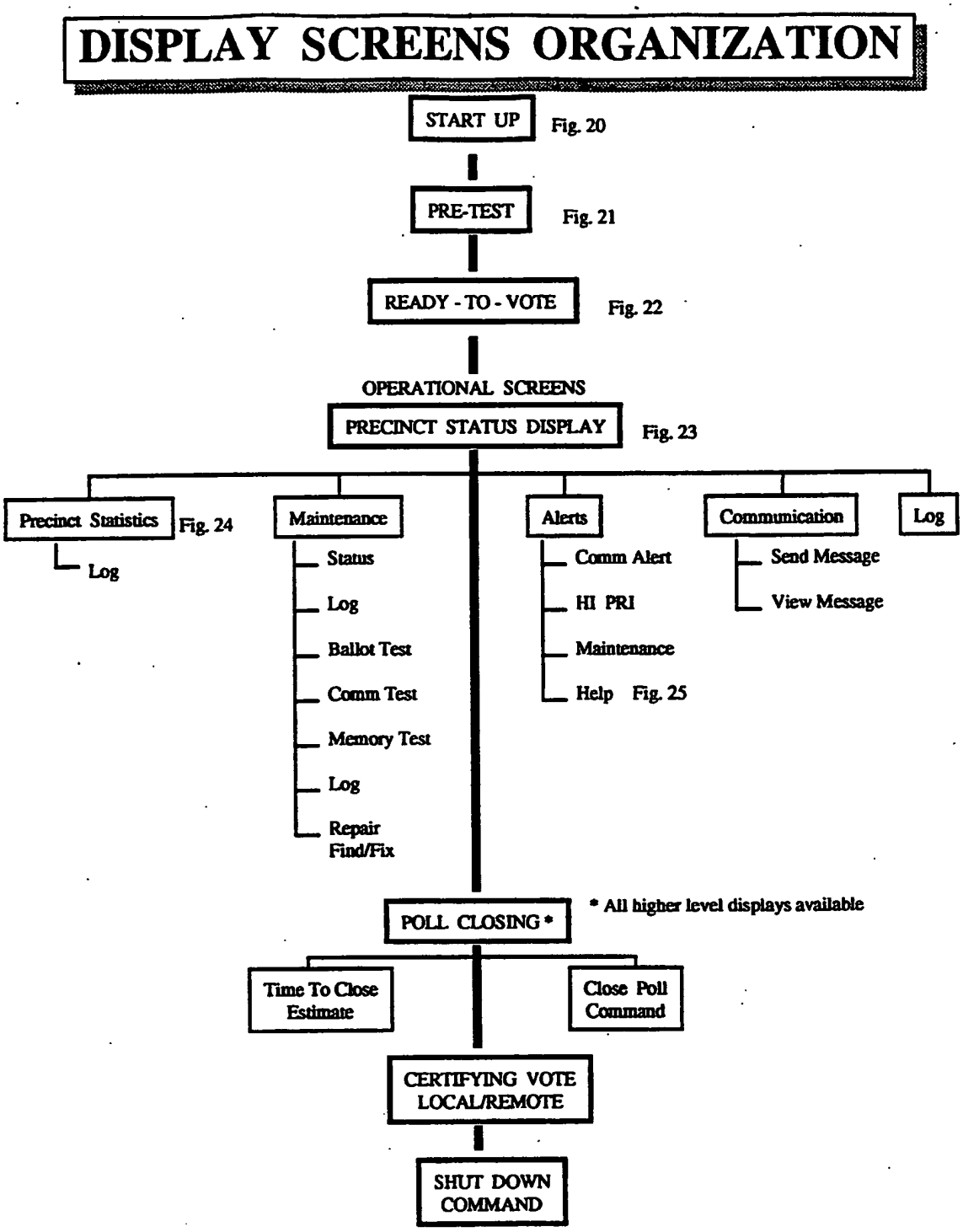


FIGURE 16 • Precinct Hierarchical Display Structure

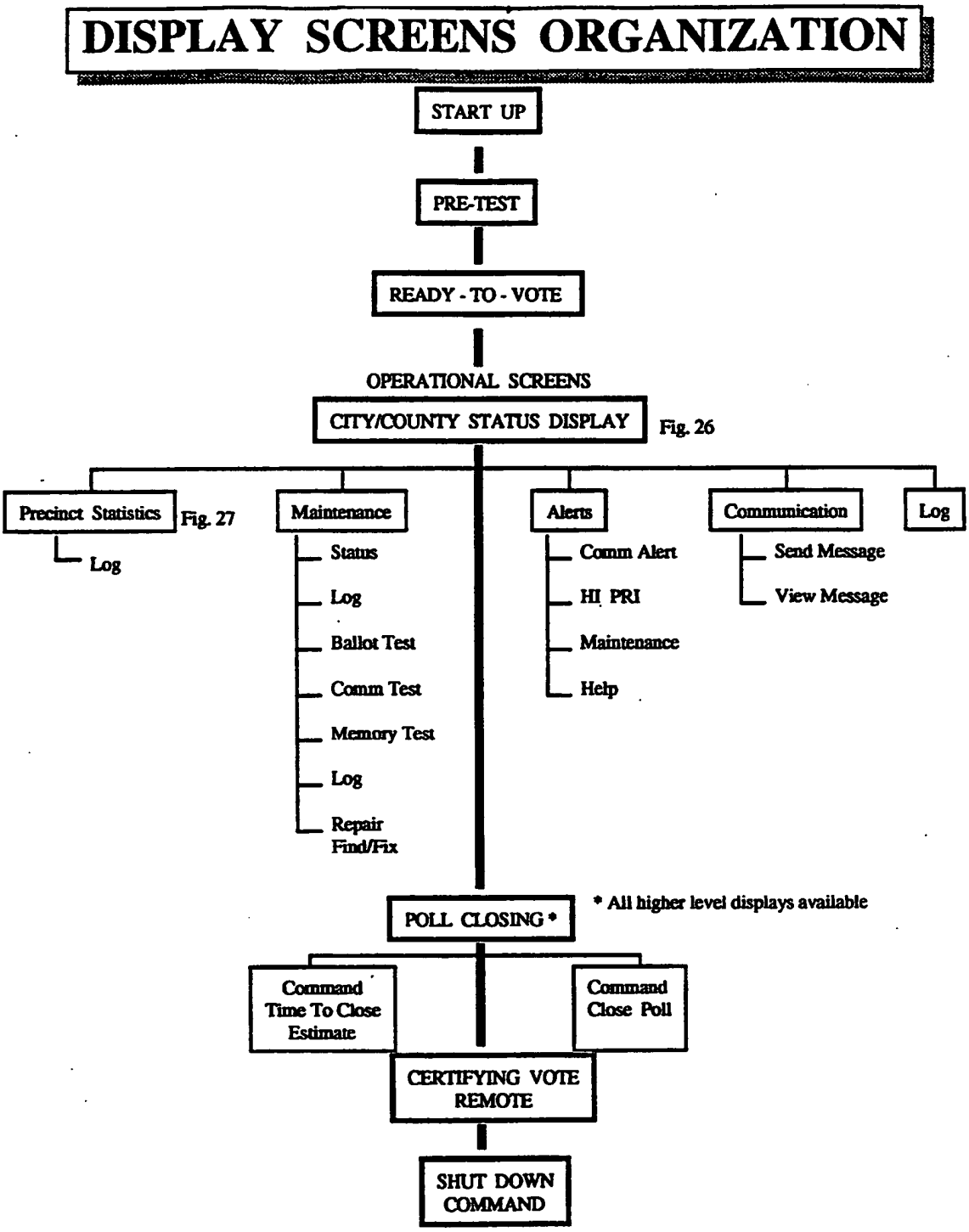


FIGURE 17 • City/County Hierarchical Display Structure

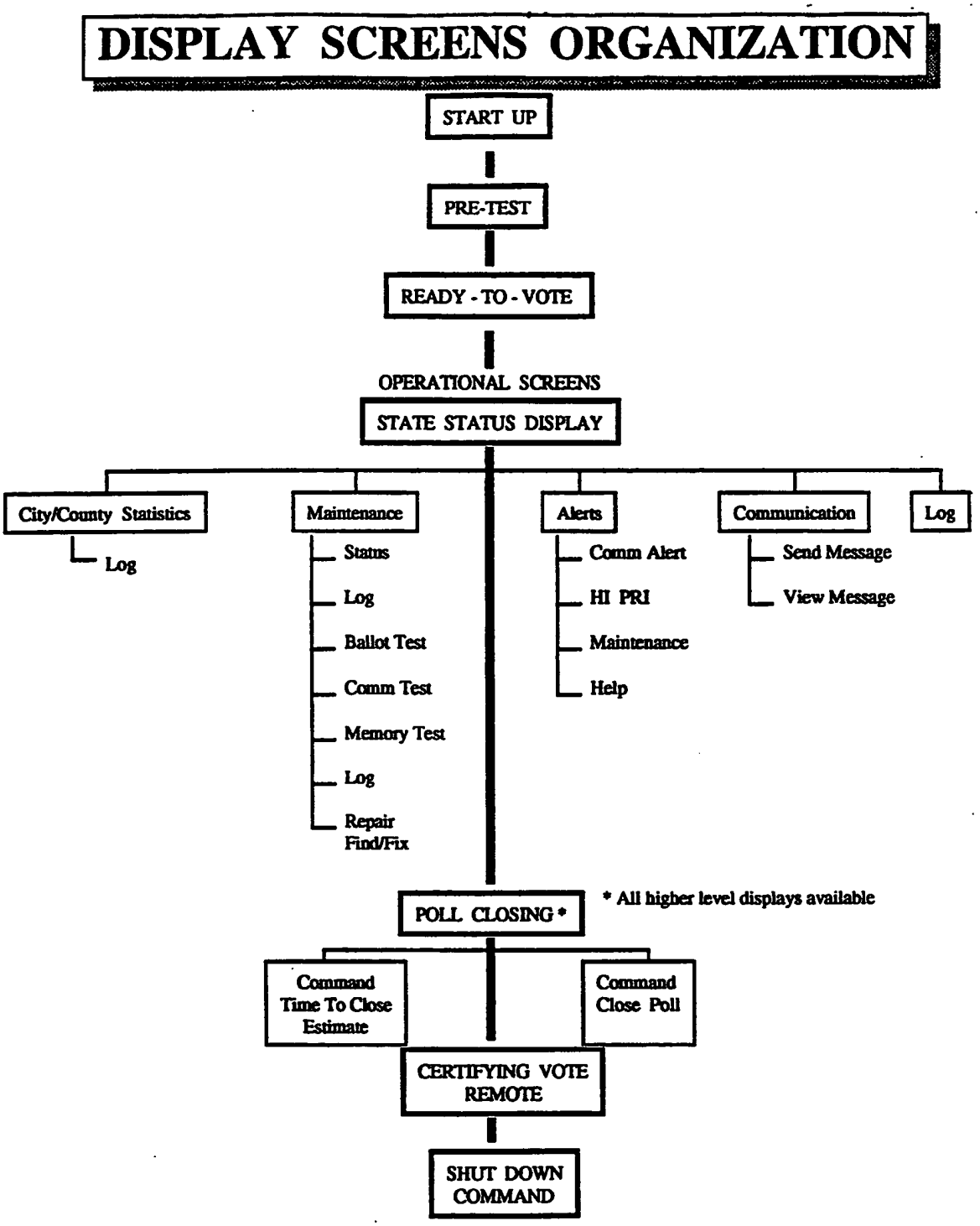


FIGURE 18 • State Hierarchical Display Structure

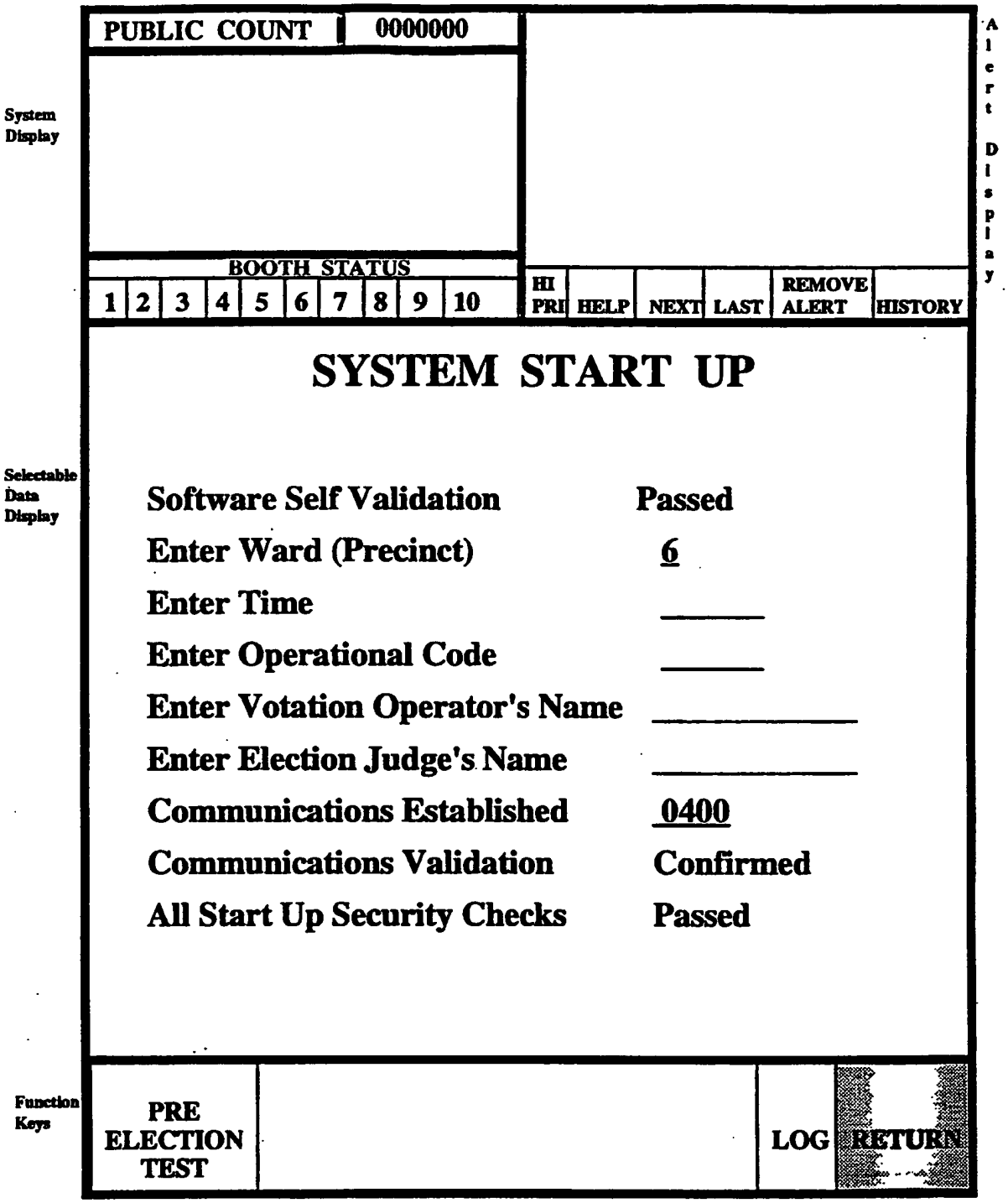


FIGURE 19 • System Start Up Screen

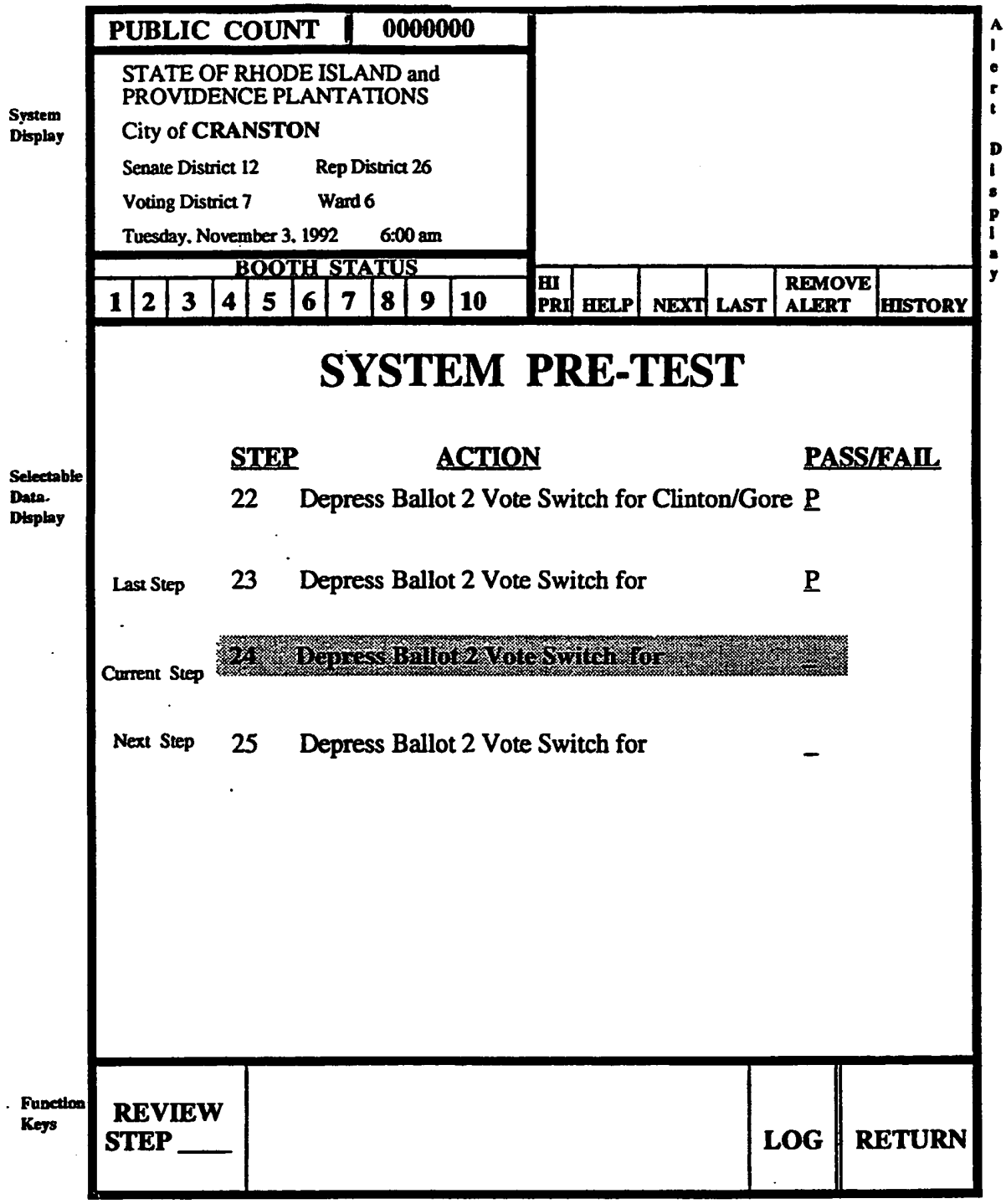


FIGURE 20 • System Pre-test

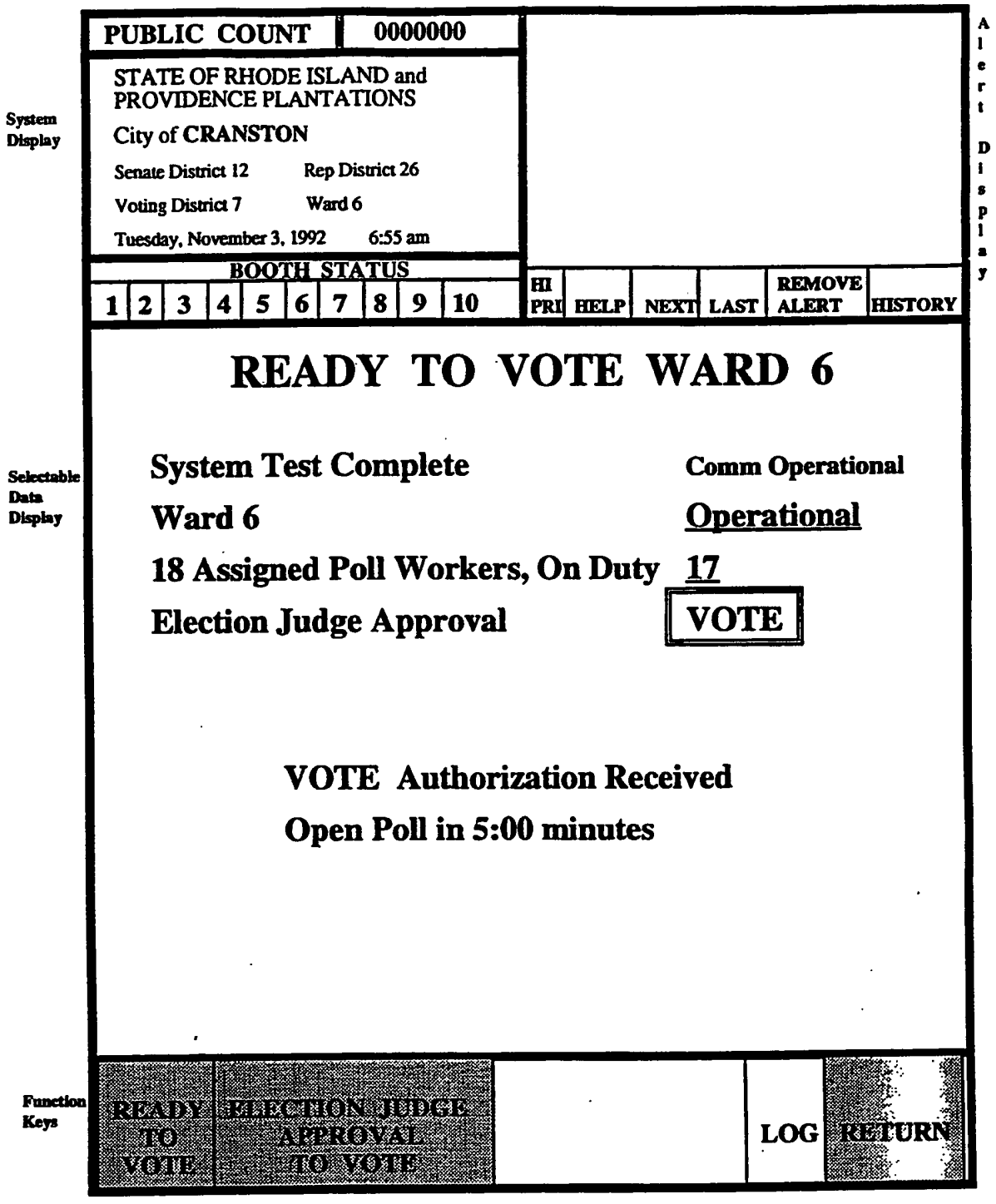


FIGURE 21 • Ready-To-Vote Display

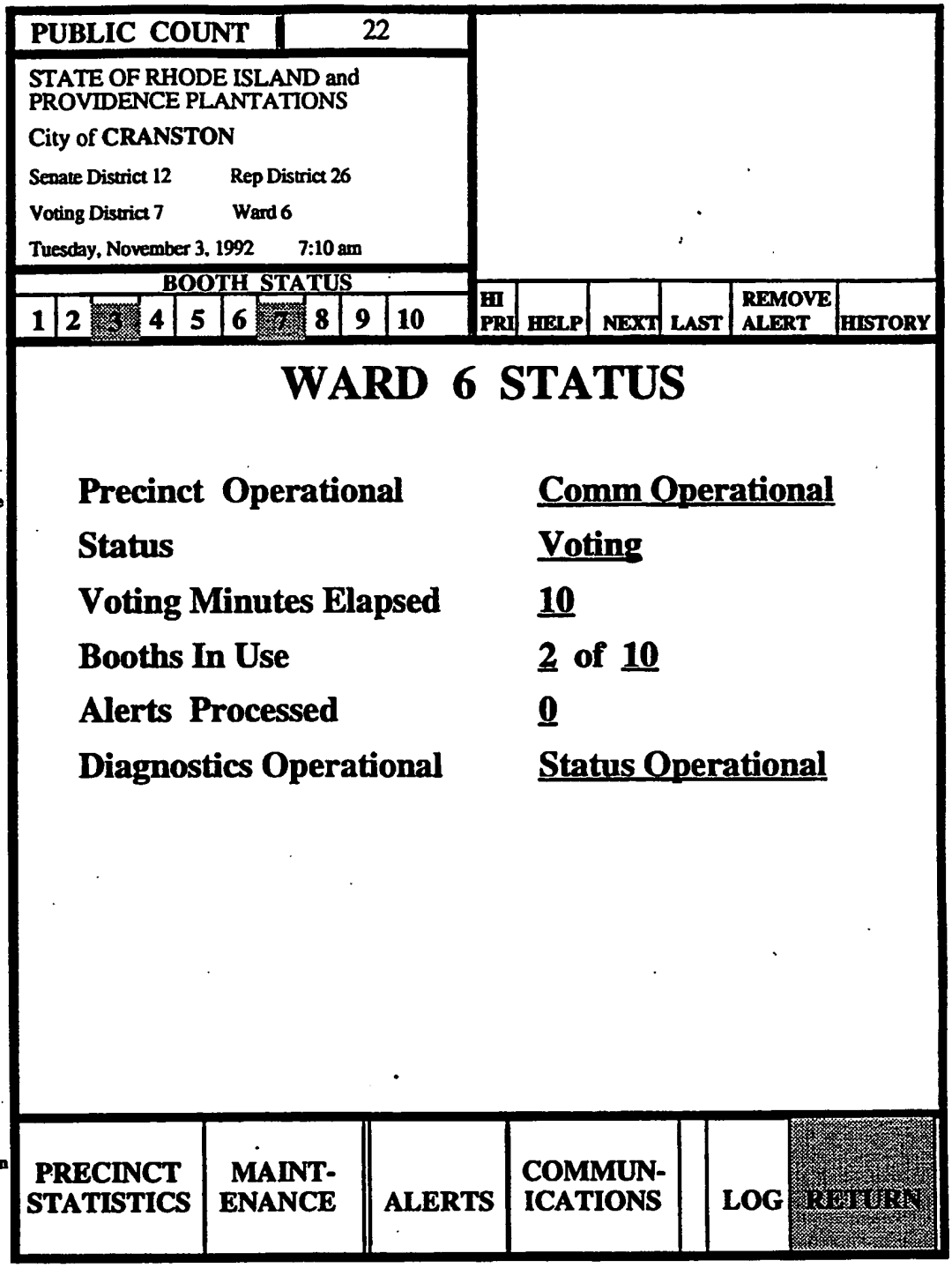


FIGURE 22 • Precinct Status Display

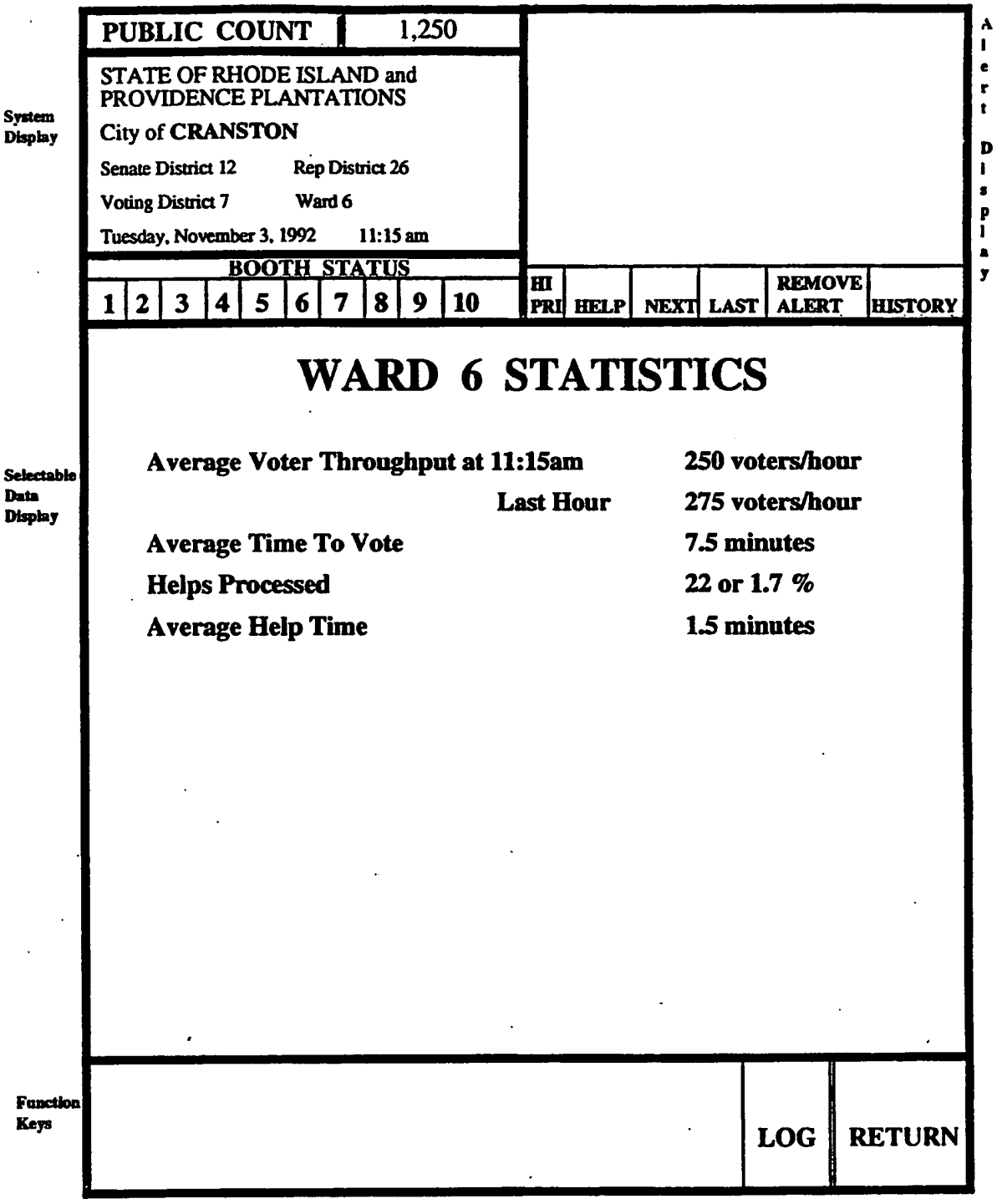


FIGURE 23 • Precinct Statistics Display

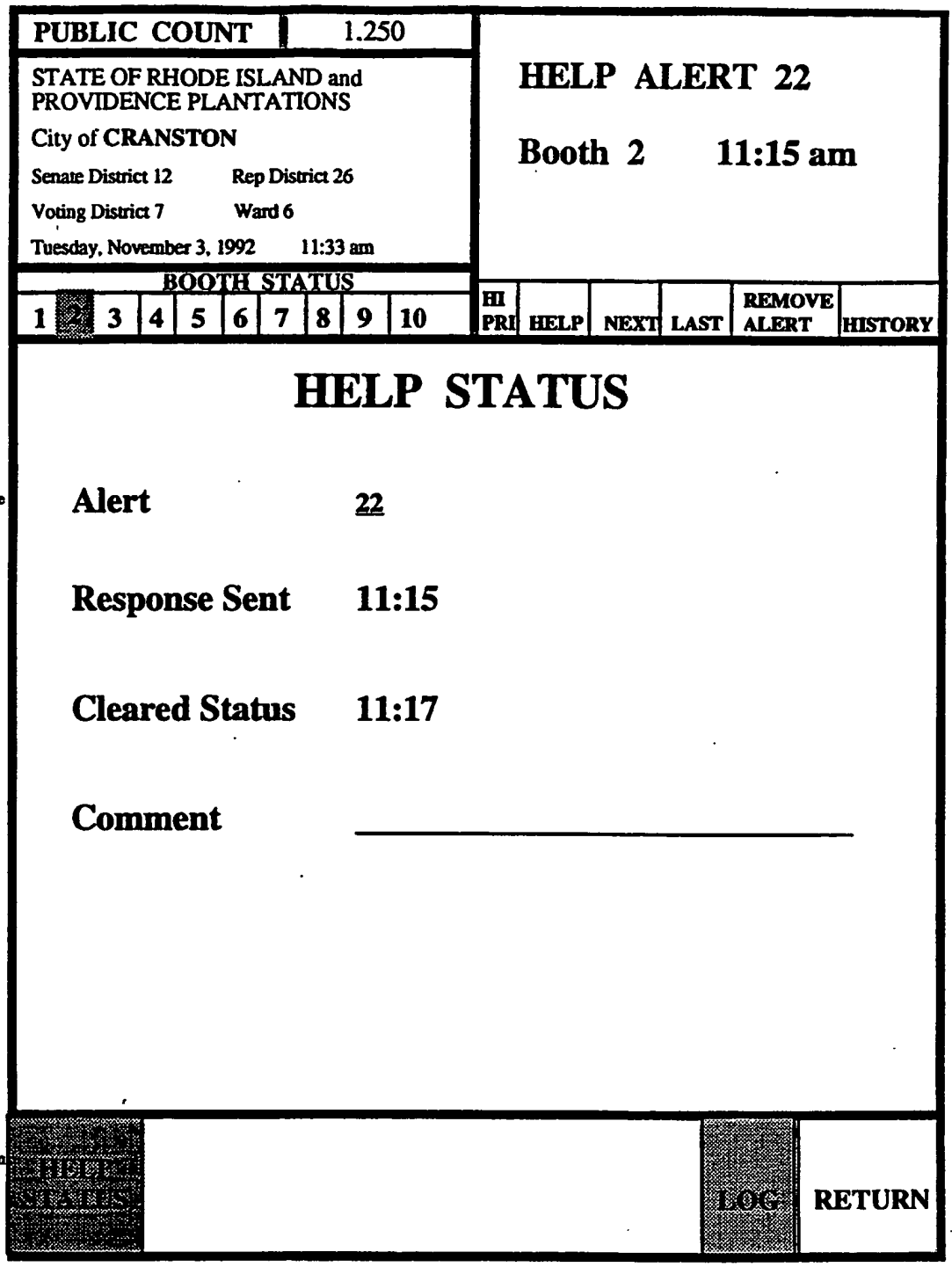


FIGURE 24 • Help Status Display

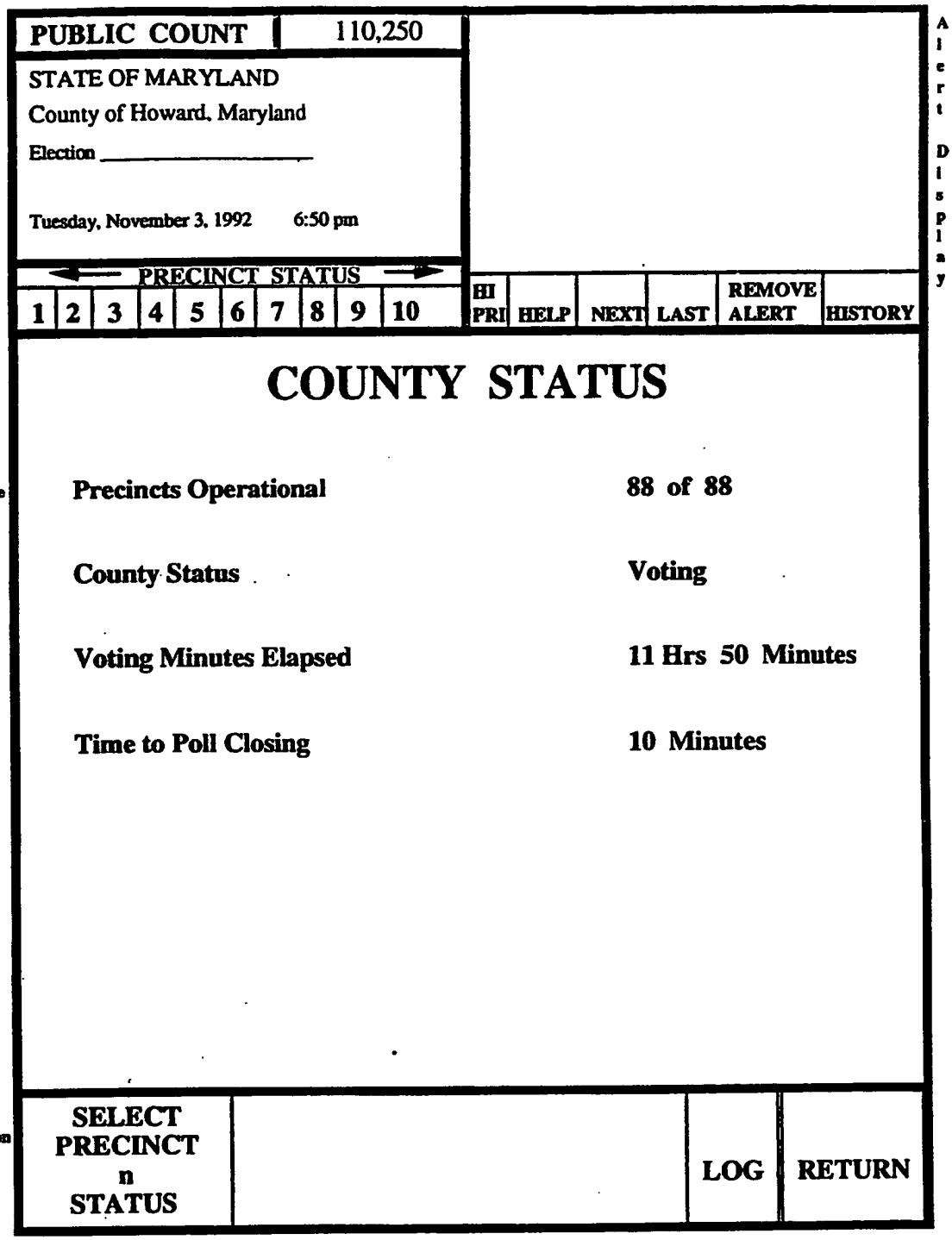


FIGURE 25 • City/County Status Display

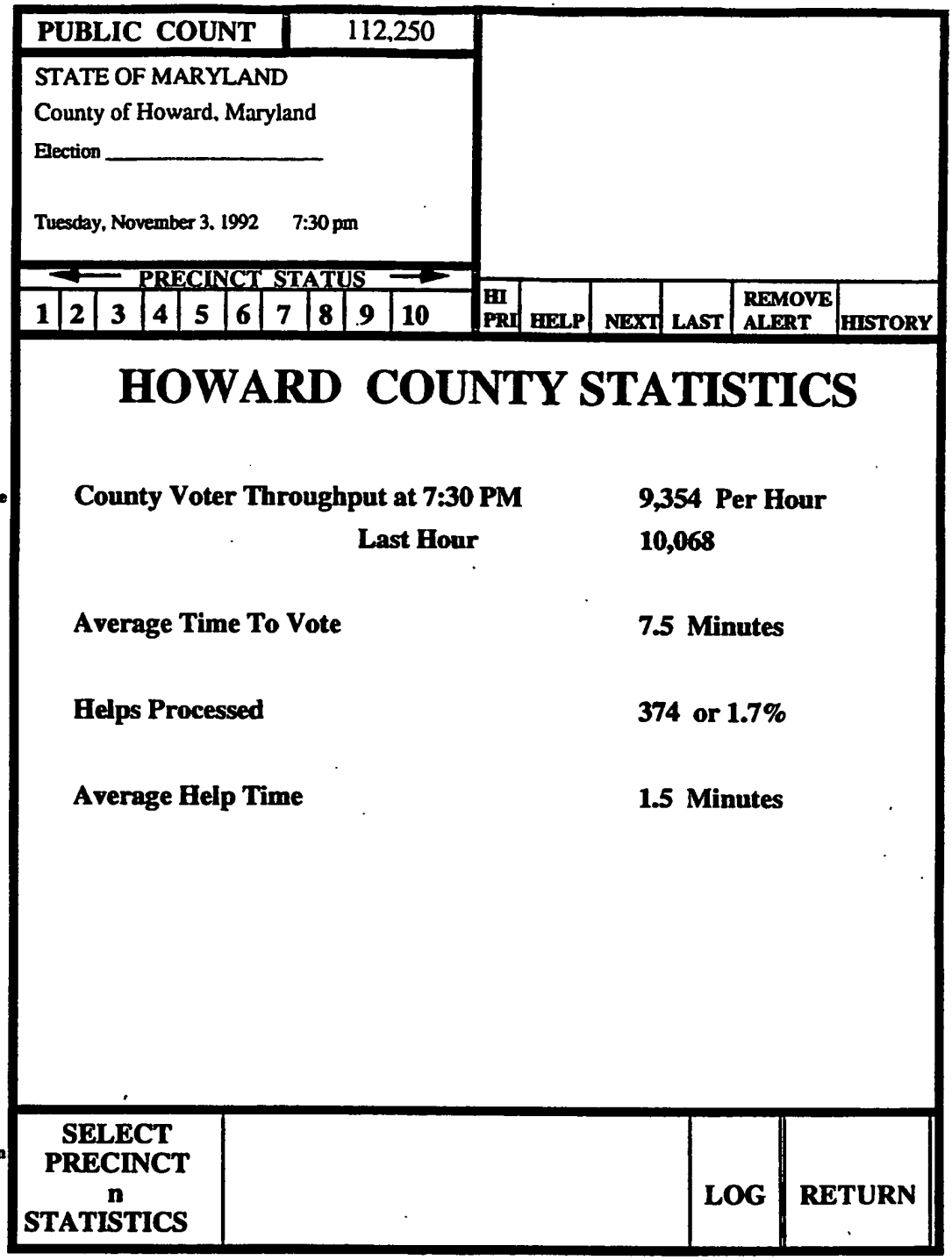


FIGURE 26 • City/County Statistics Display

System Display

PUBLIC COUNT	2,579

STATE OF MARYLAND
County of Howard, Maryland
Election _____

Tuesday, November 3, 1992 9:10 am

Alert Display

PRECINCT STATUS

1	2	3	4	5	6	7	8	9	10

HI PRI	HELP	NEXT	LAST	REMOVE ALERT	HISTORY

PRECINCT 8 STATUS

Selectable Data Display

Precinct 8	Operational
Poll Workers Present	10 of 10
System Operator	J. Johnson
Chief Poll Judge	F. Smith
Poll Opened	7:00 am
Precinct 8 Public Count at 9:10 am	2,579

Function Keys

STATUS	STATISTICS	PRECINCT NUMBER		LOG	RETURN

FIGURE 27 • Select Precinct Display

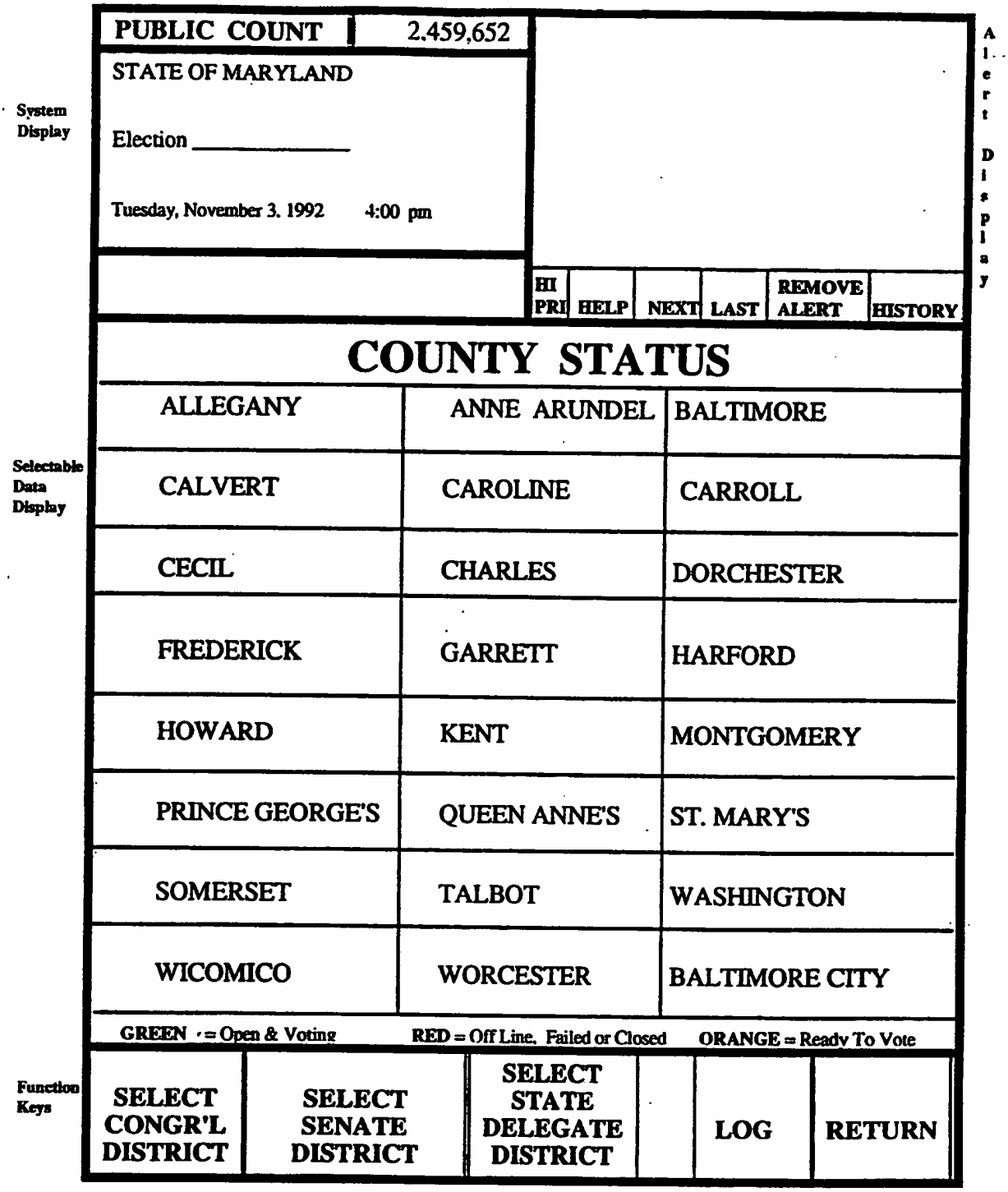


FIGURE 28 • County Status Display

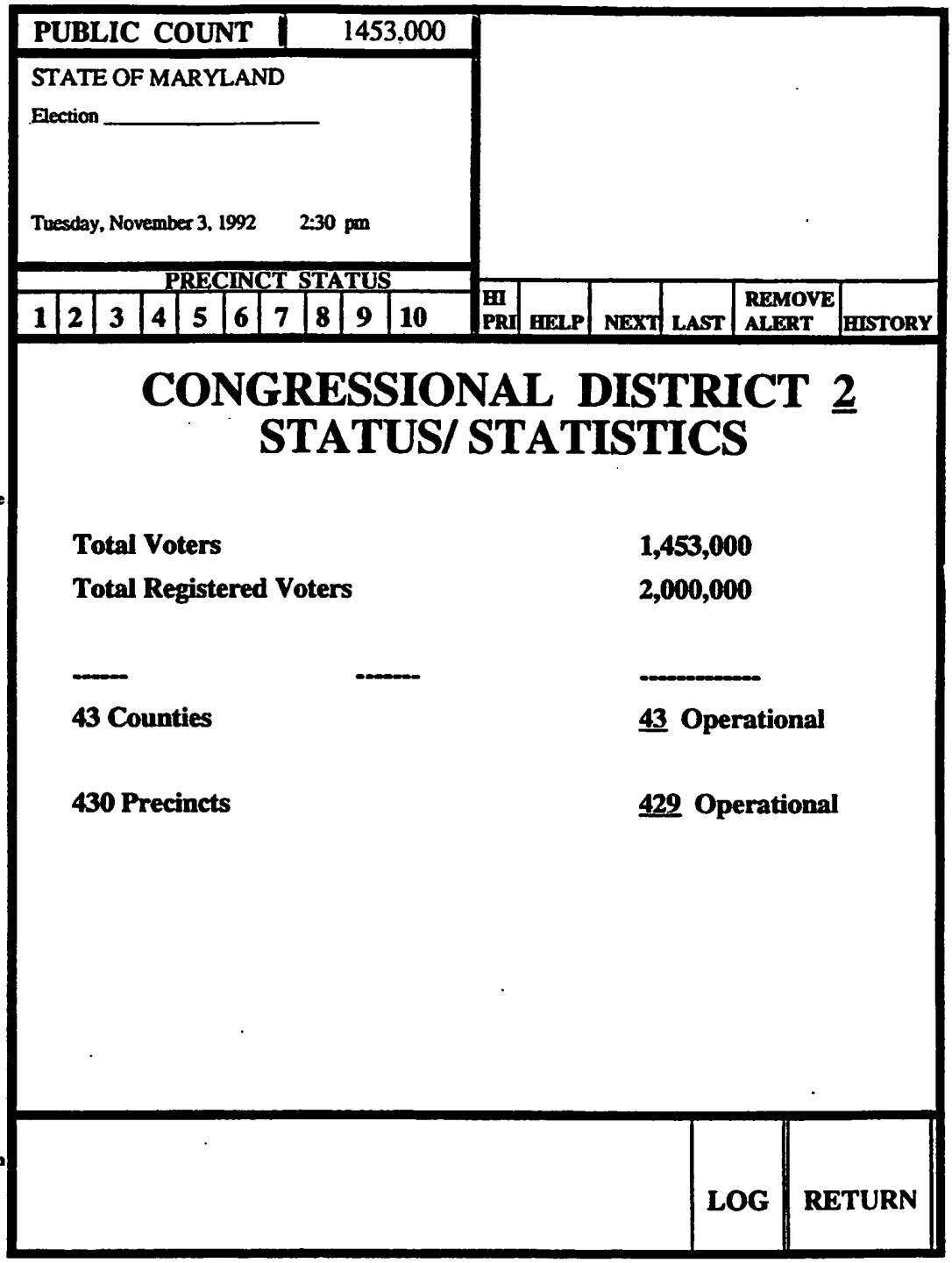
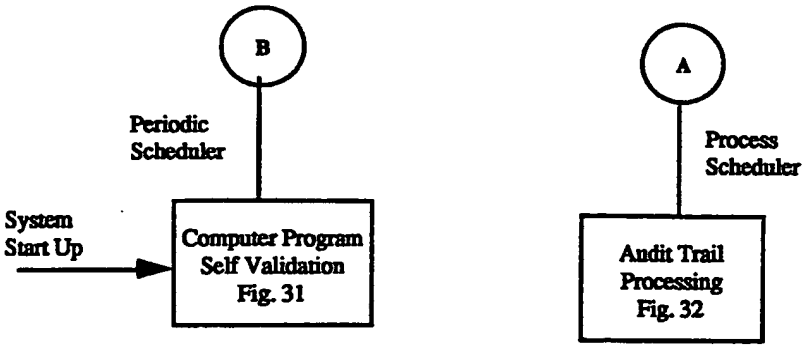


FIGURE 29 • District Based Statistics Display



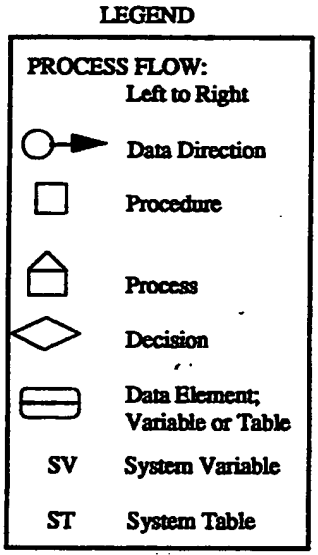


FIGURE 30 • Common Logical Processing Functions

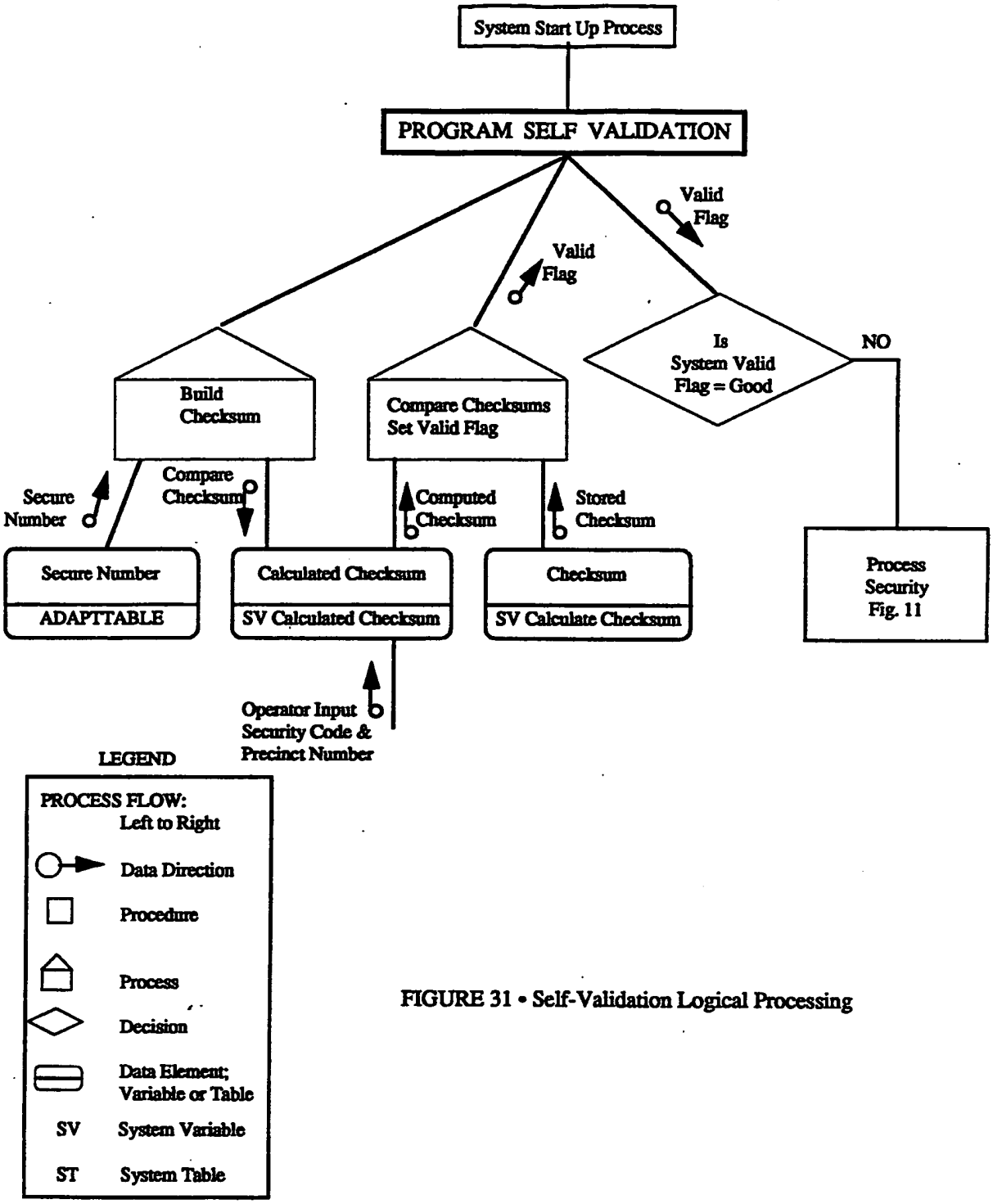


FIGURE 31 • Self-Validation Logical Processing

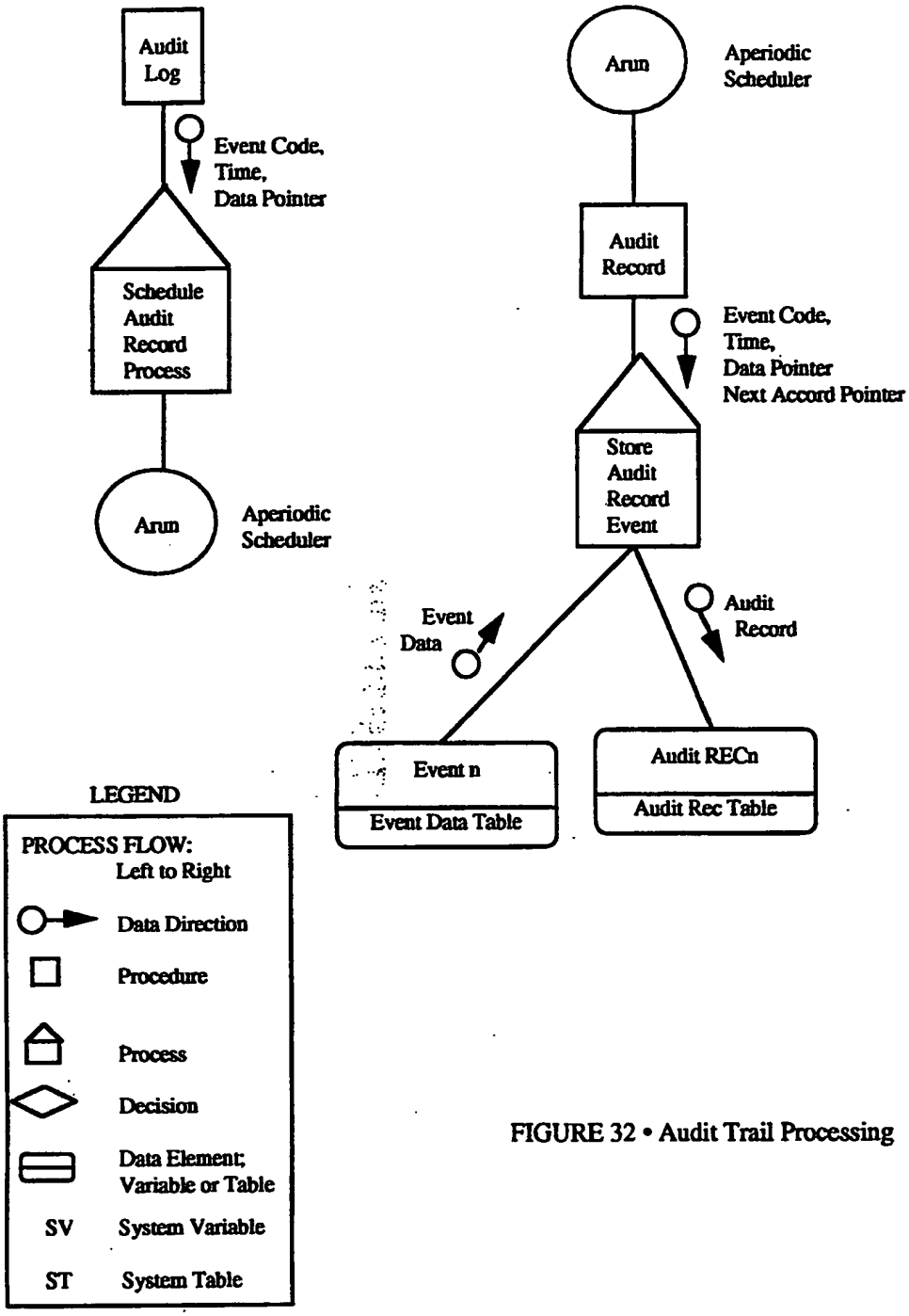


FIGURE 32 • Audit Trail Processing

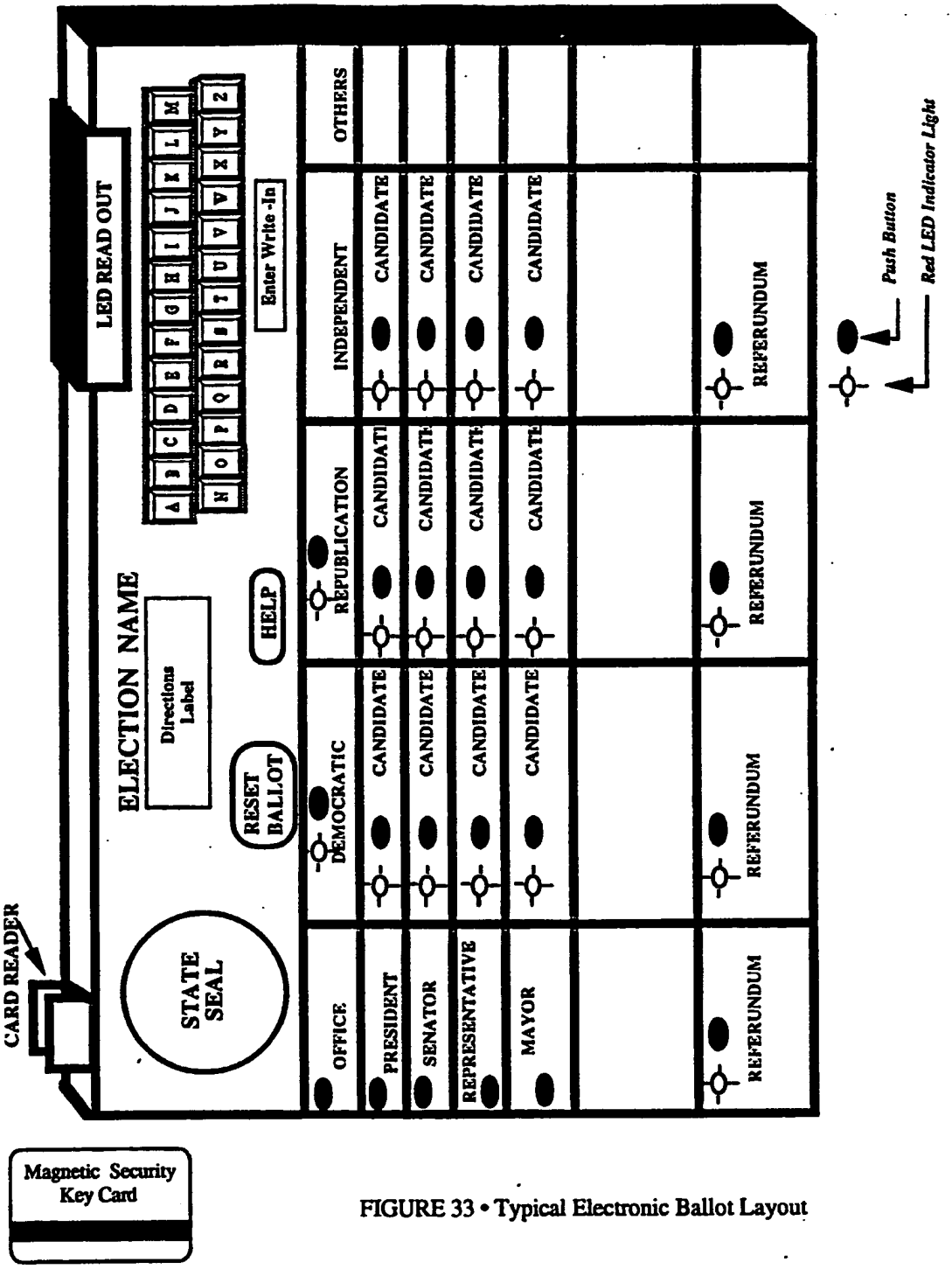


FIGURE 33 • Typical Electronic Ballot Layout

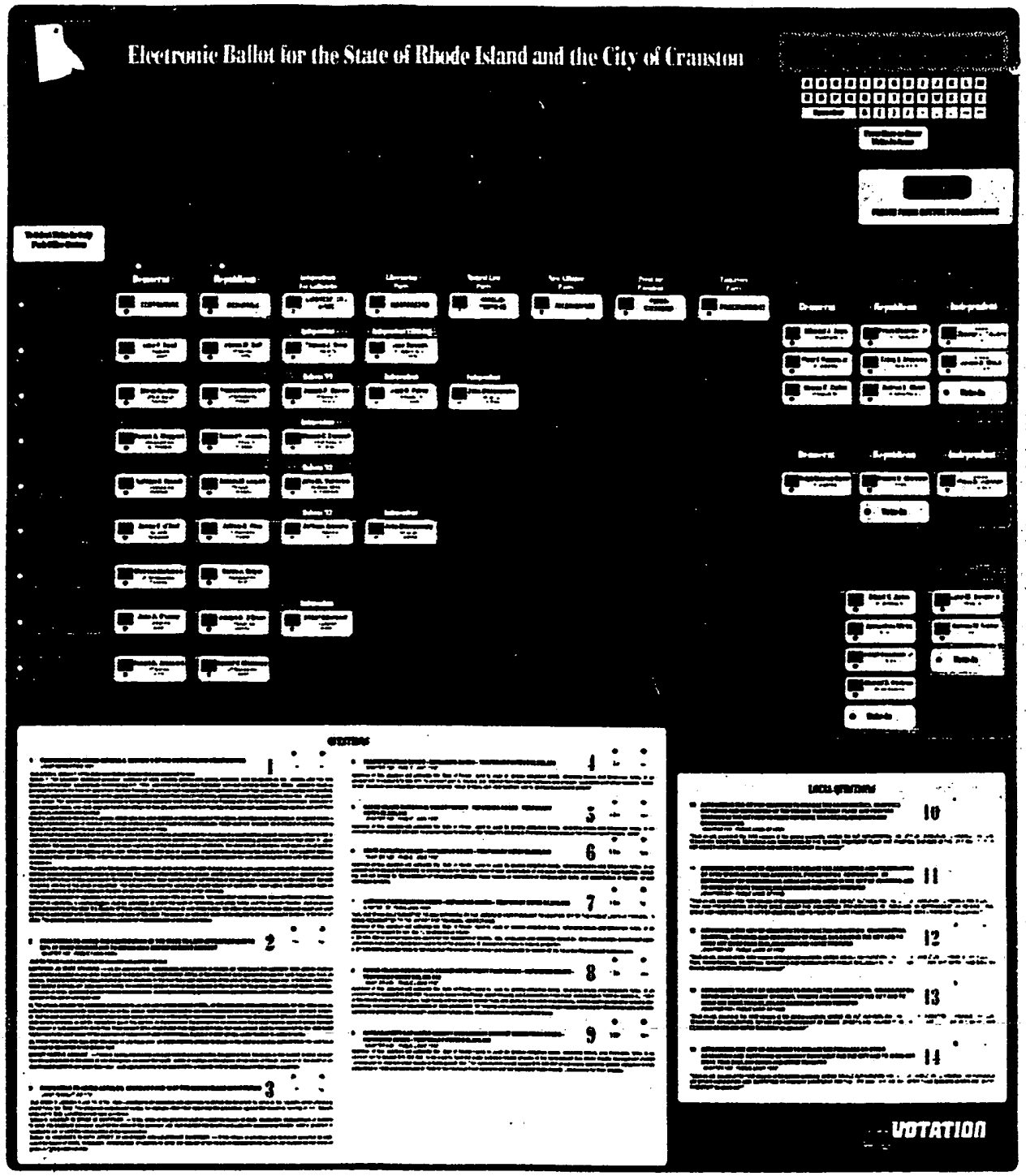


FIGURE 3 Rhode Island Sample Ballot

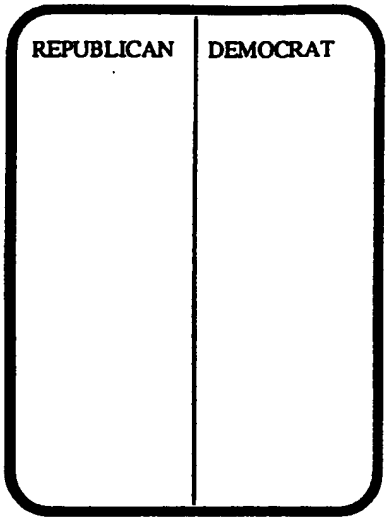


FIGURE 35 • Split Ballot

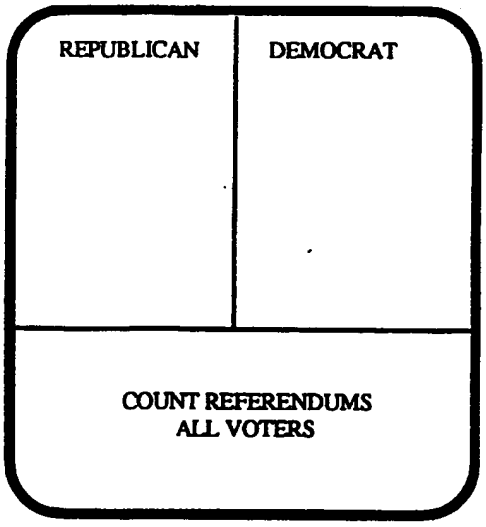


FIGURE 36 • Split Ballot with Common Referendum Issues

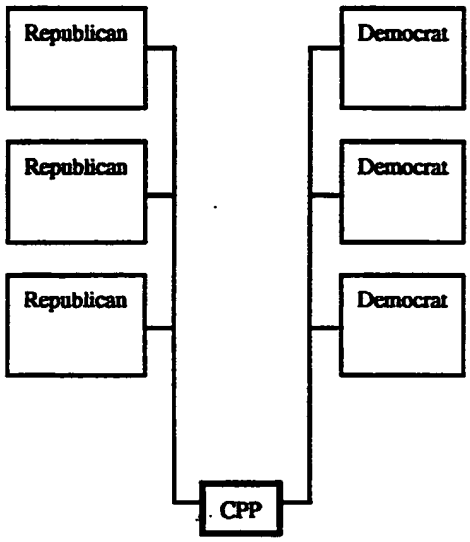


FIGURE 37• Split Precinct Ballot Configuration

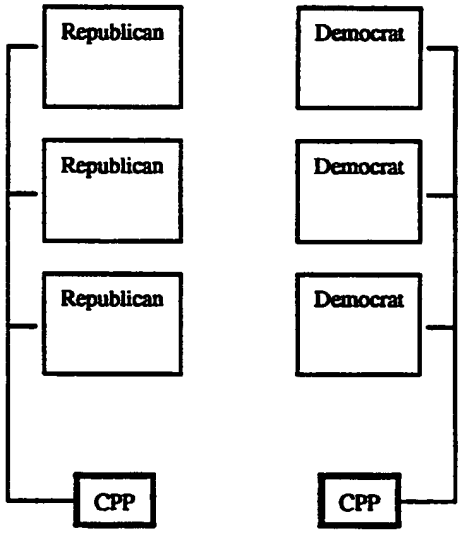


FIGURE 38 • Split Precinct System Configuration

Primary Election-Ballot Style & Configuration Options

This Page Blank (uspto)

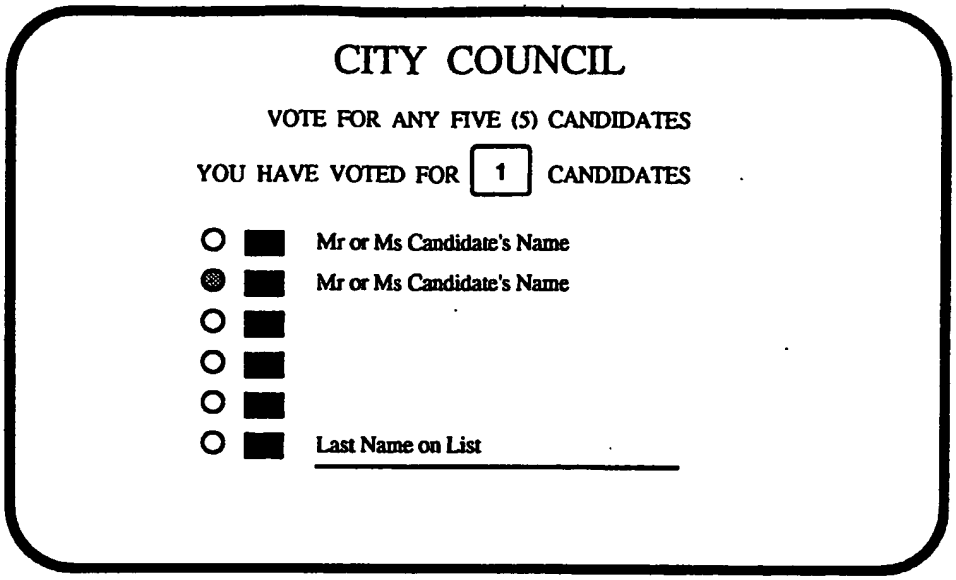


FIGURE 39 • Multi- Vote Race Ballot with Vote Counter

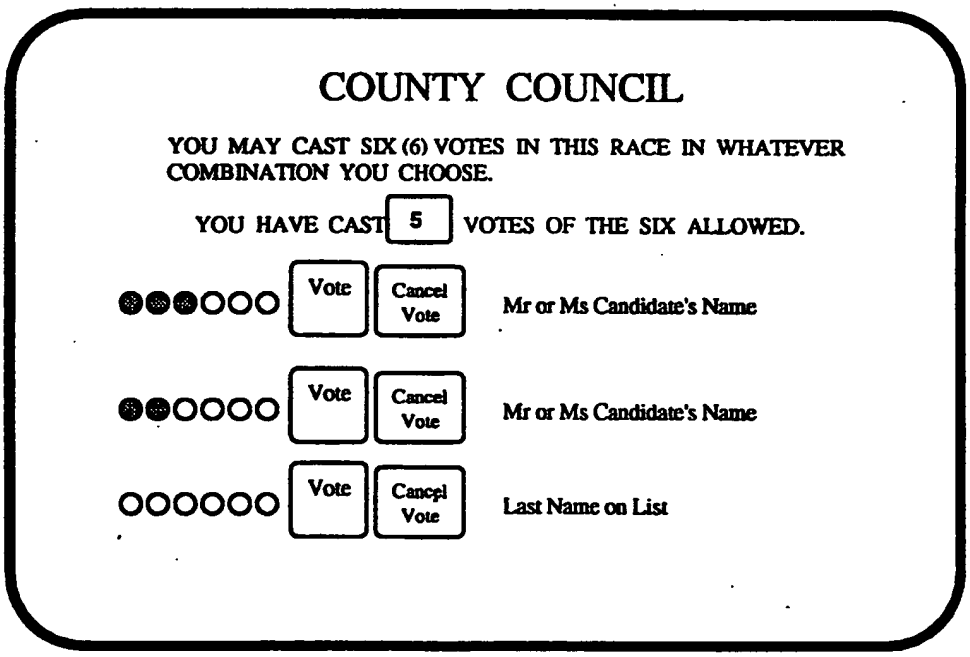


FIGURE 40 • Multi-Vote Race with Multi-Votes Per Candidate Allowed

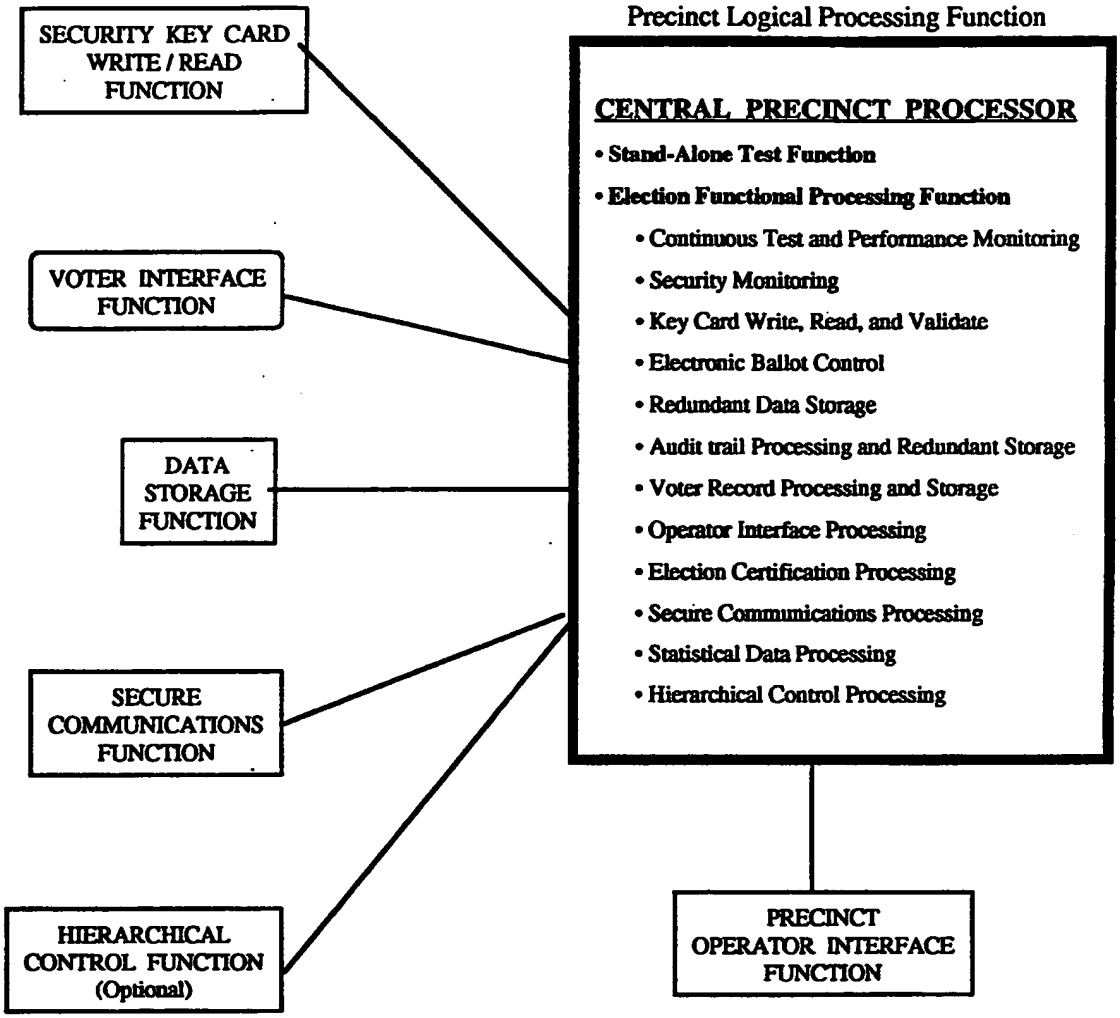


FIGURE 41 • Central Precinct Processor Functional Block Diagram

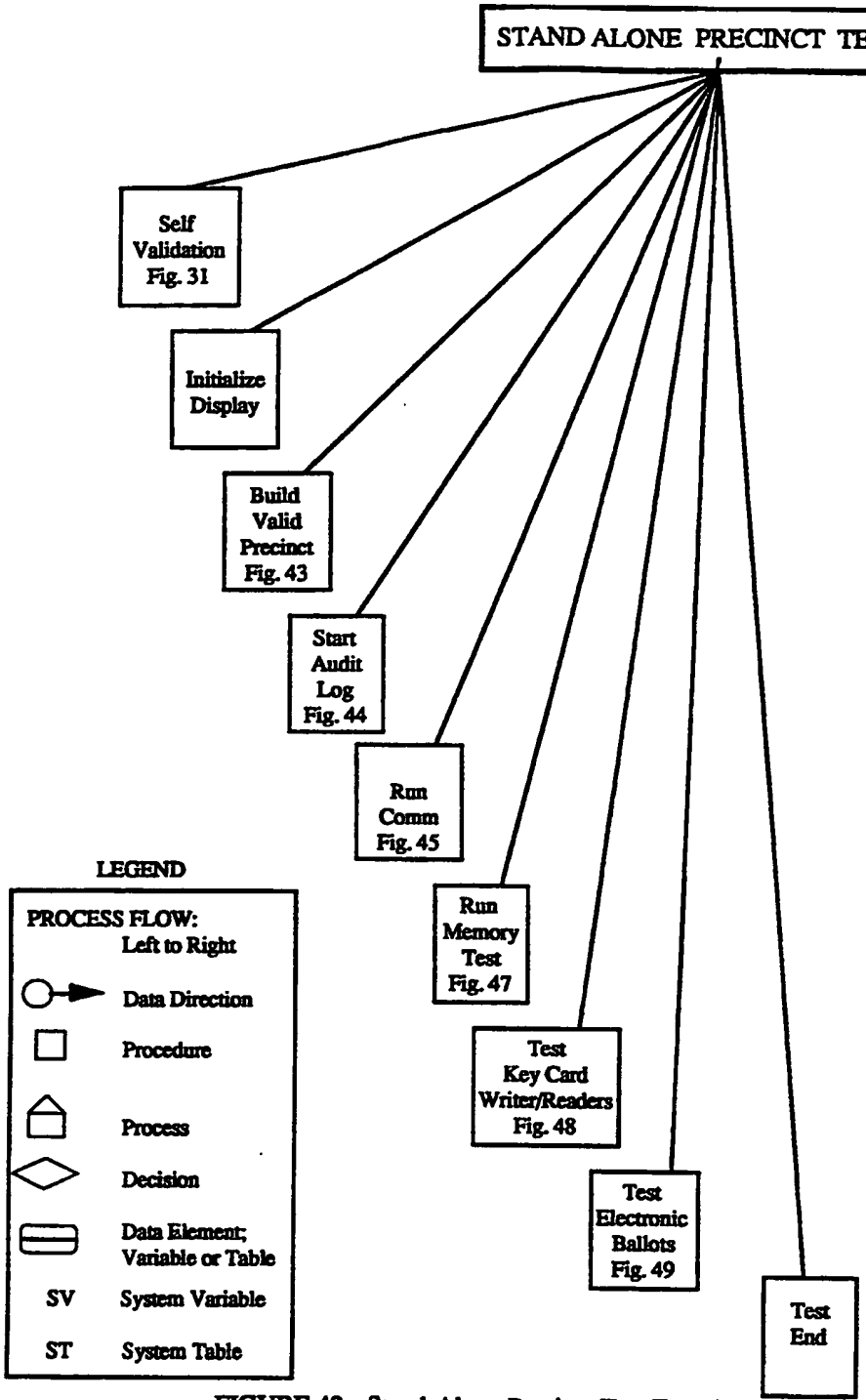
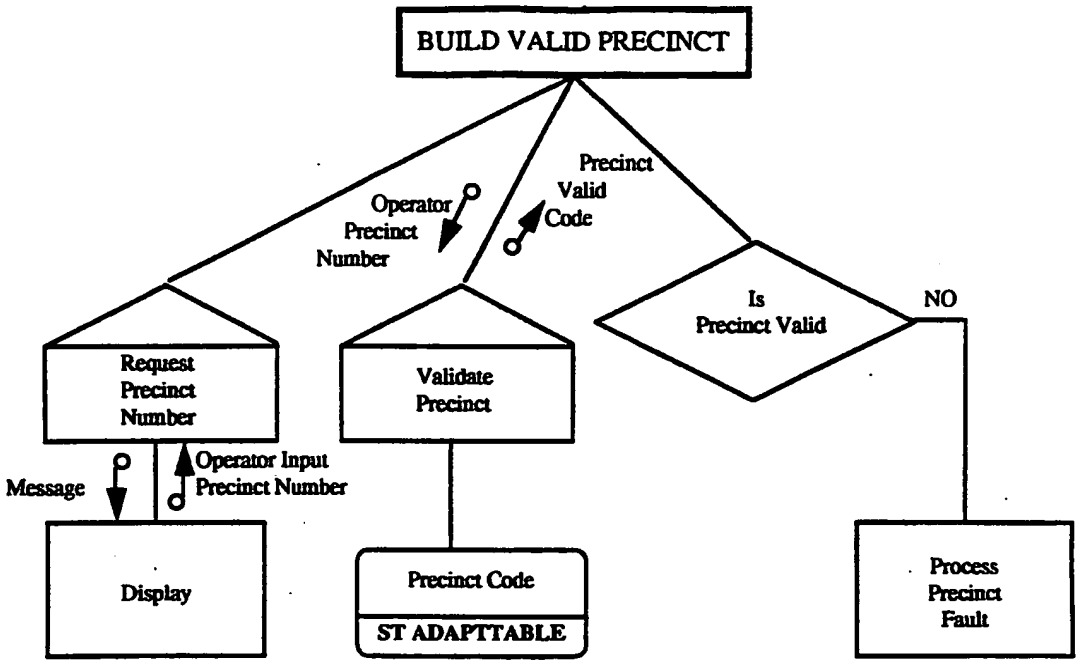


FIGURE 42 • Stand-Alone Precinct Test Function



Adaptation Parameter Table

ST ADAPTTABLE	
Precinct State/County Code	MD, Howard, 22
Ballots	10
Input Matrix Pointer	1,000
Comm	Yes
Full control	Yes
Modified Controllable Pointer	0
Input Switch Matrix	
0,0 = Clinton/Gore	
Switch 0,1 =	
Switch 0,2 =	
Switch 0,3 =	
Switch 0,4 =	
Switch 1,0 =	
Switch 1,1 =	
Switch 1,2 =	
Switch 1,3 =	
Switch 1,4 =	

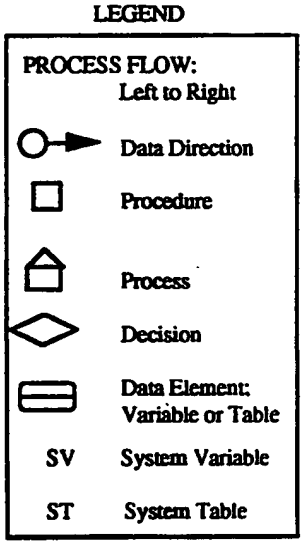
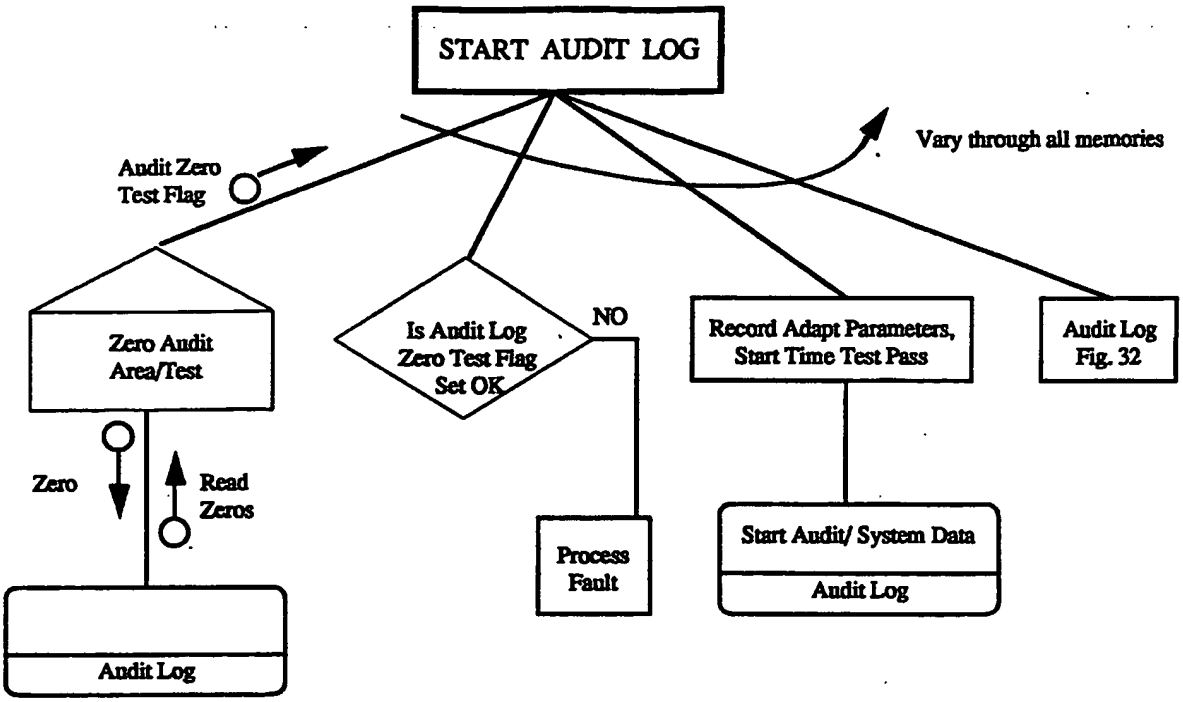


FIGURE 43 • Build Valid Precinct



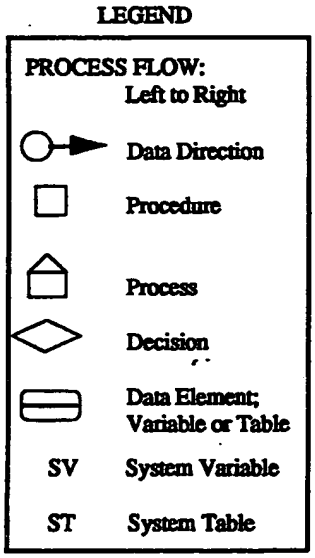
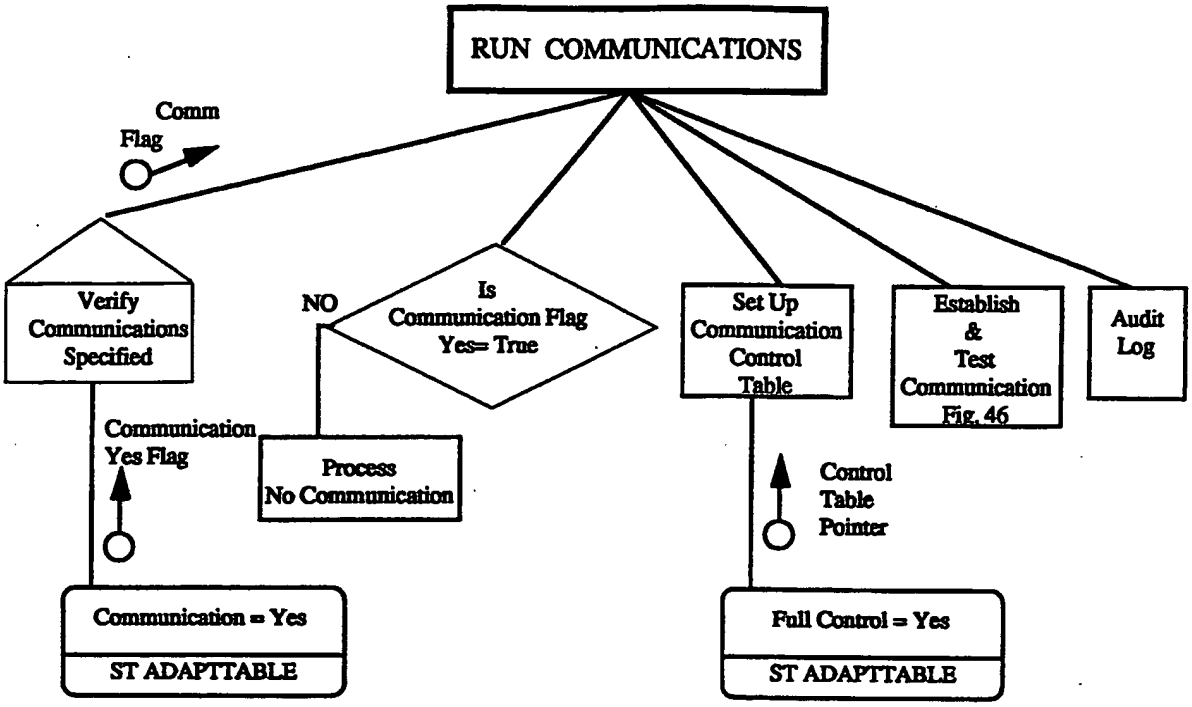


FIGURE 44 • Start Audit Log



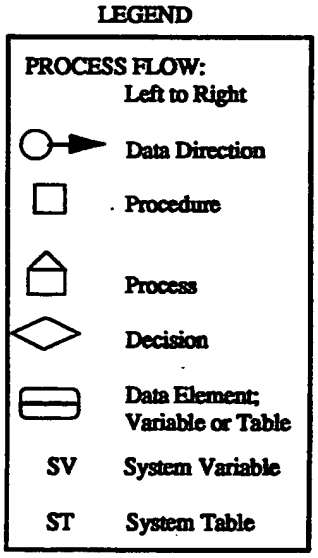
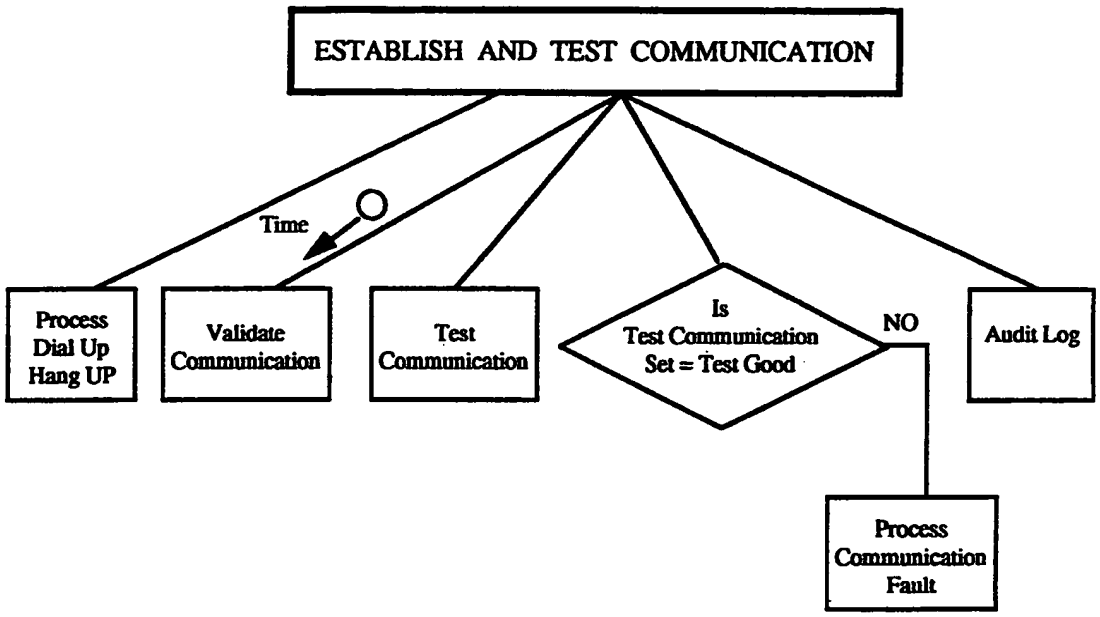


FIGURE 45 • Run Communications



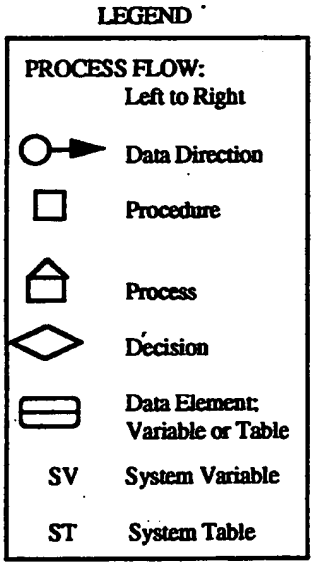


FIGURE 46 • Establish and Test Communication

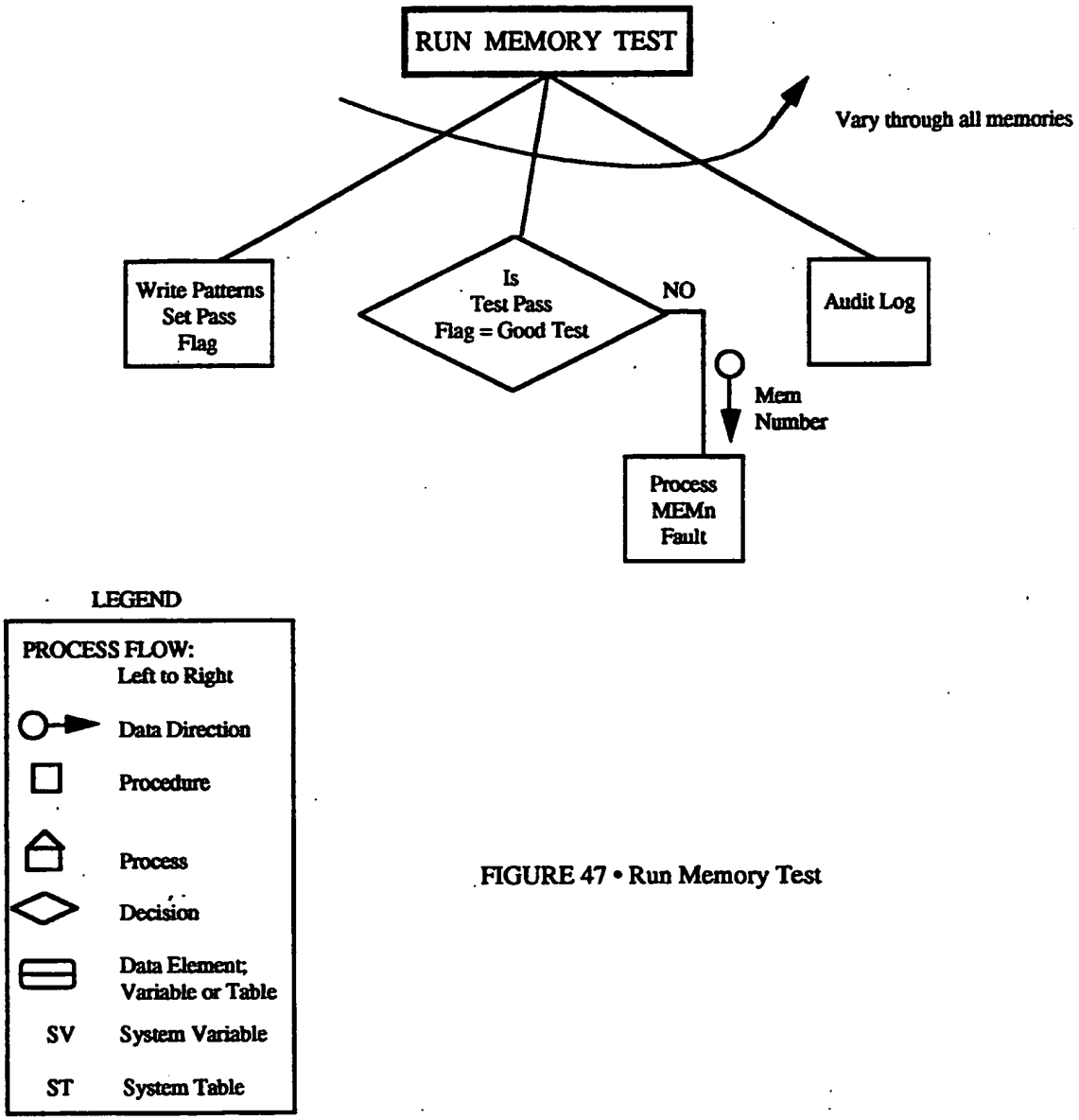


FIGURE 47 • Run Memory Test

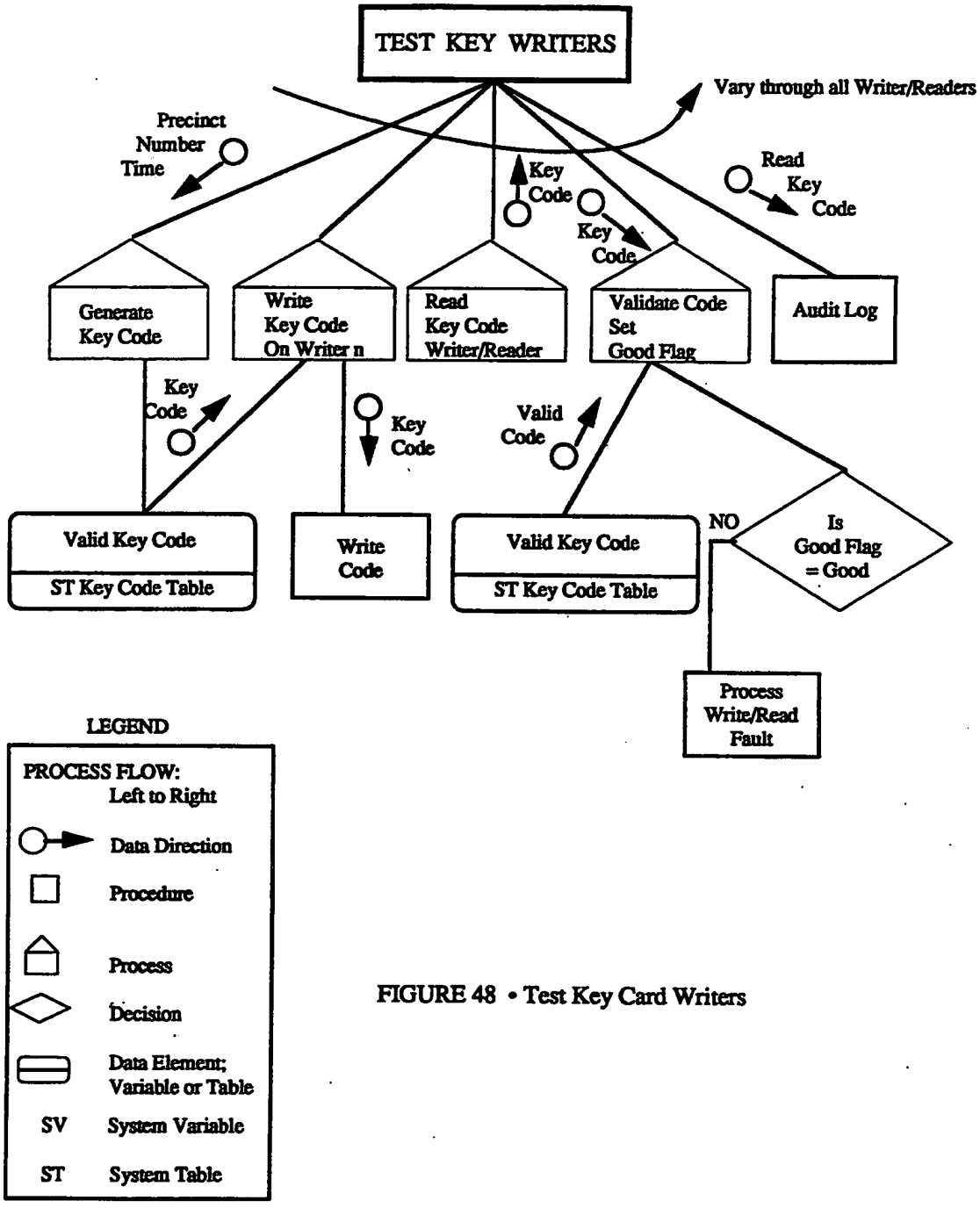
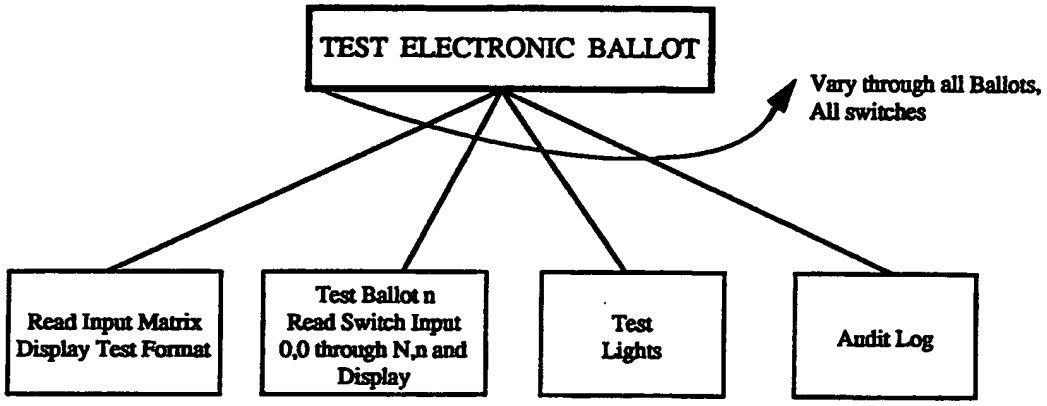


FIGURE 48 • Test Key Card Writers



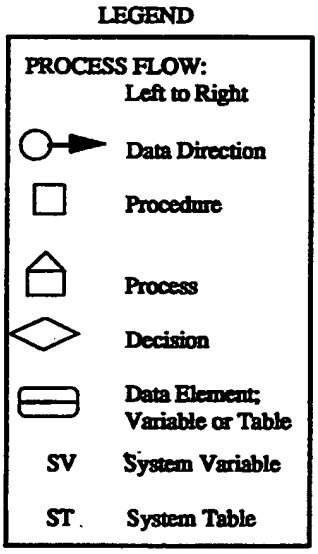


FIGURE 49 • Test Electronic Ballot

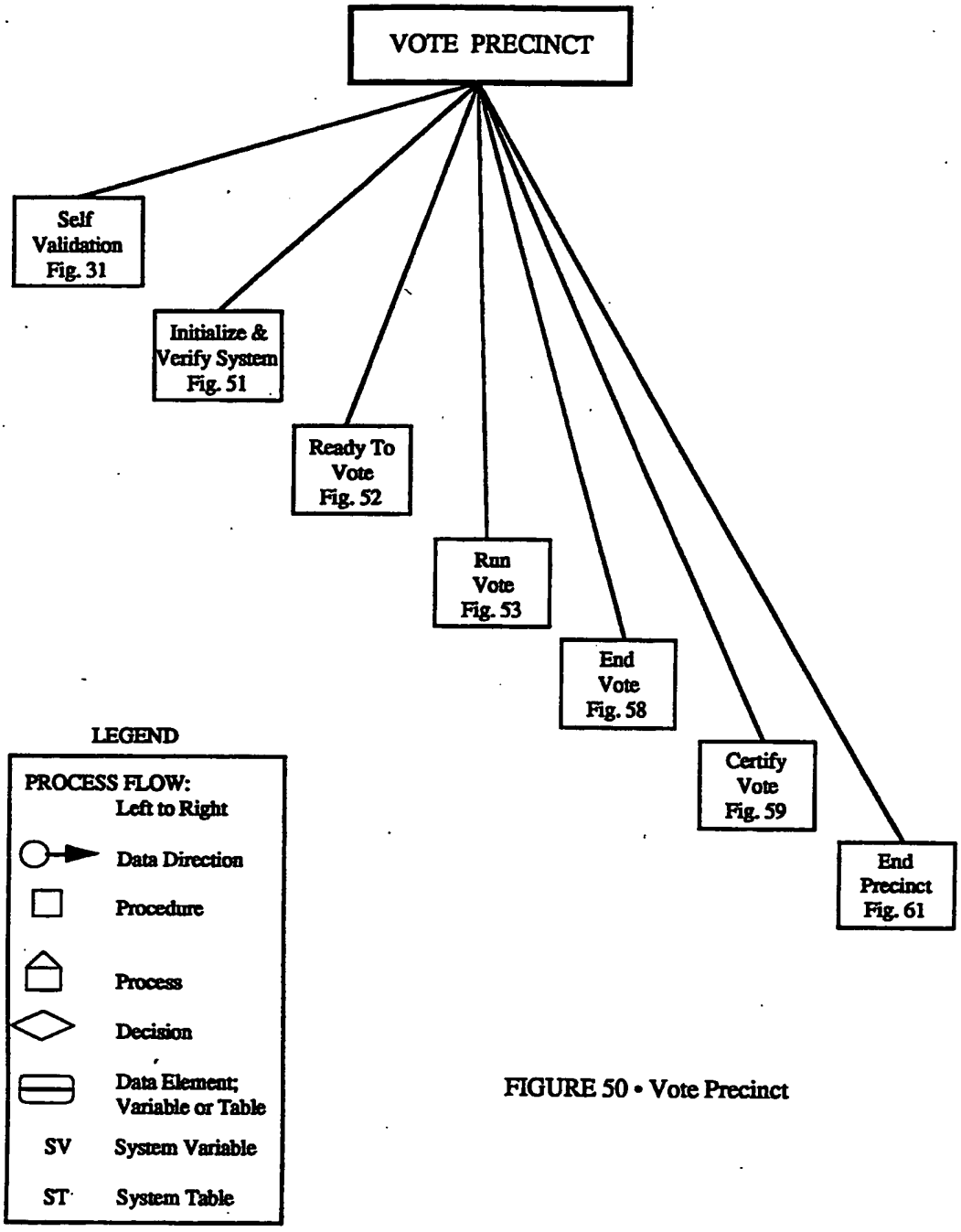


FIGURE 50 • Vote Precinct

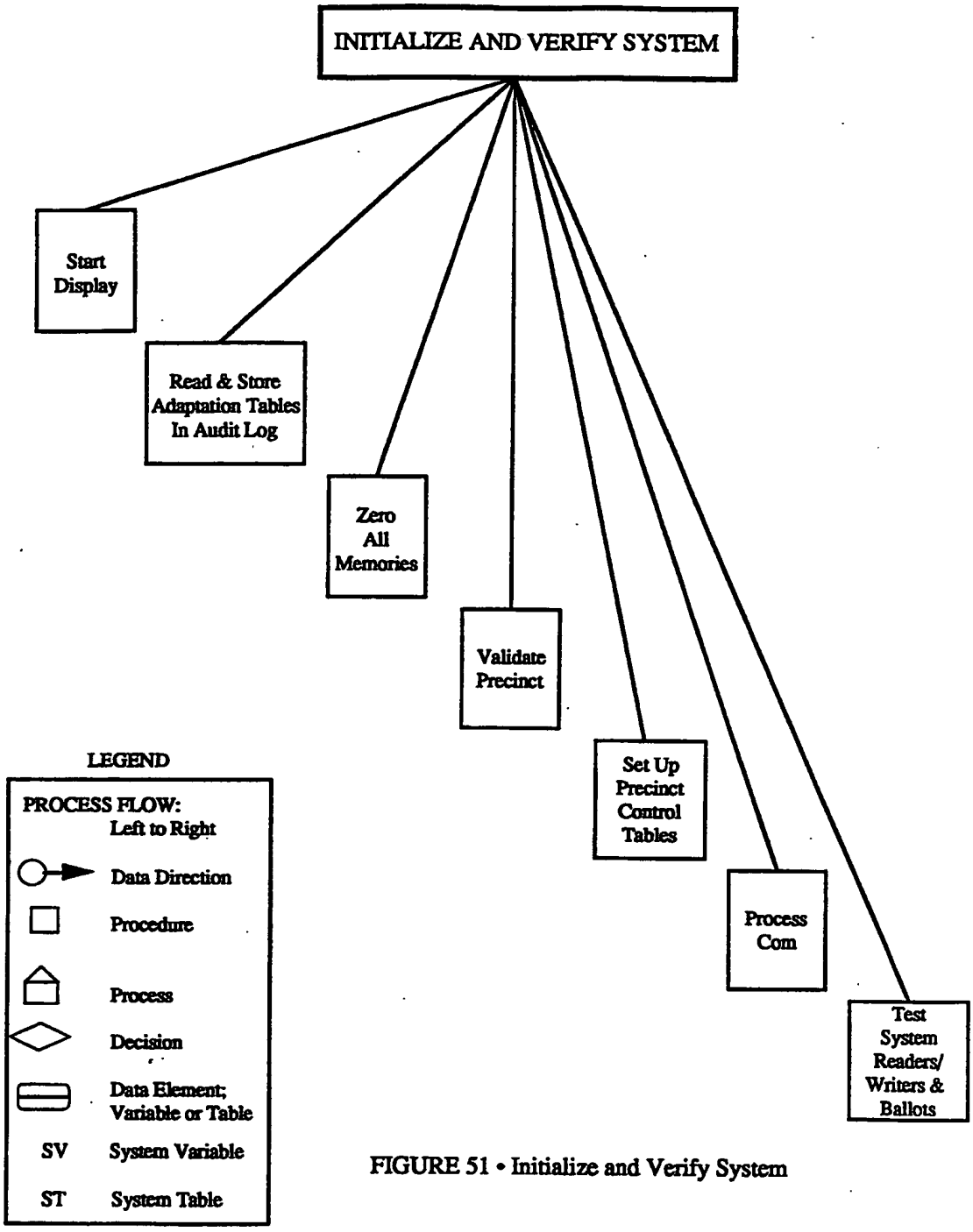
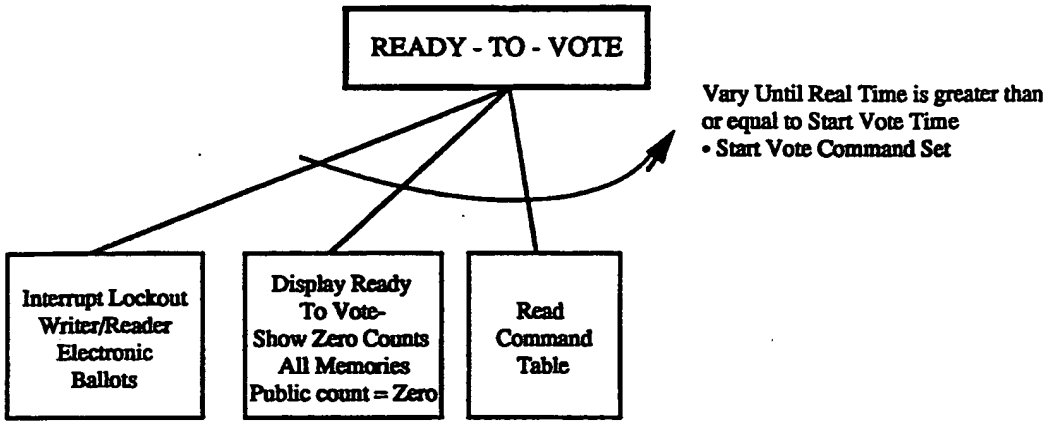


FIGURE 51 • Initialize and Verify System



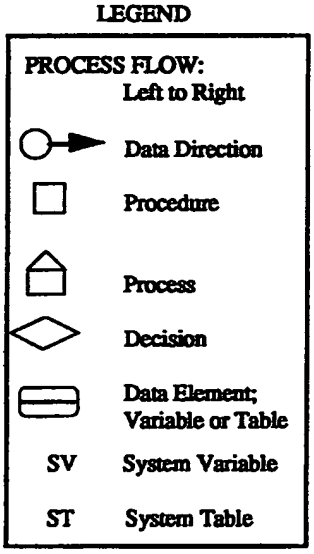
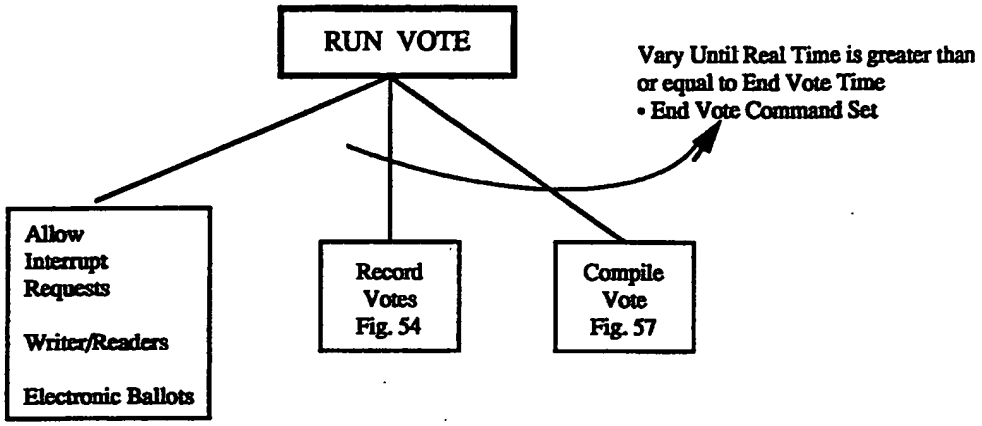


FIGURE 52 • Ready -To-Vote



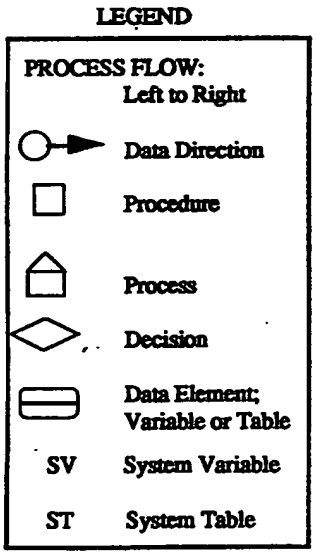


FIGURE 53 • Run Vote

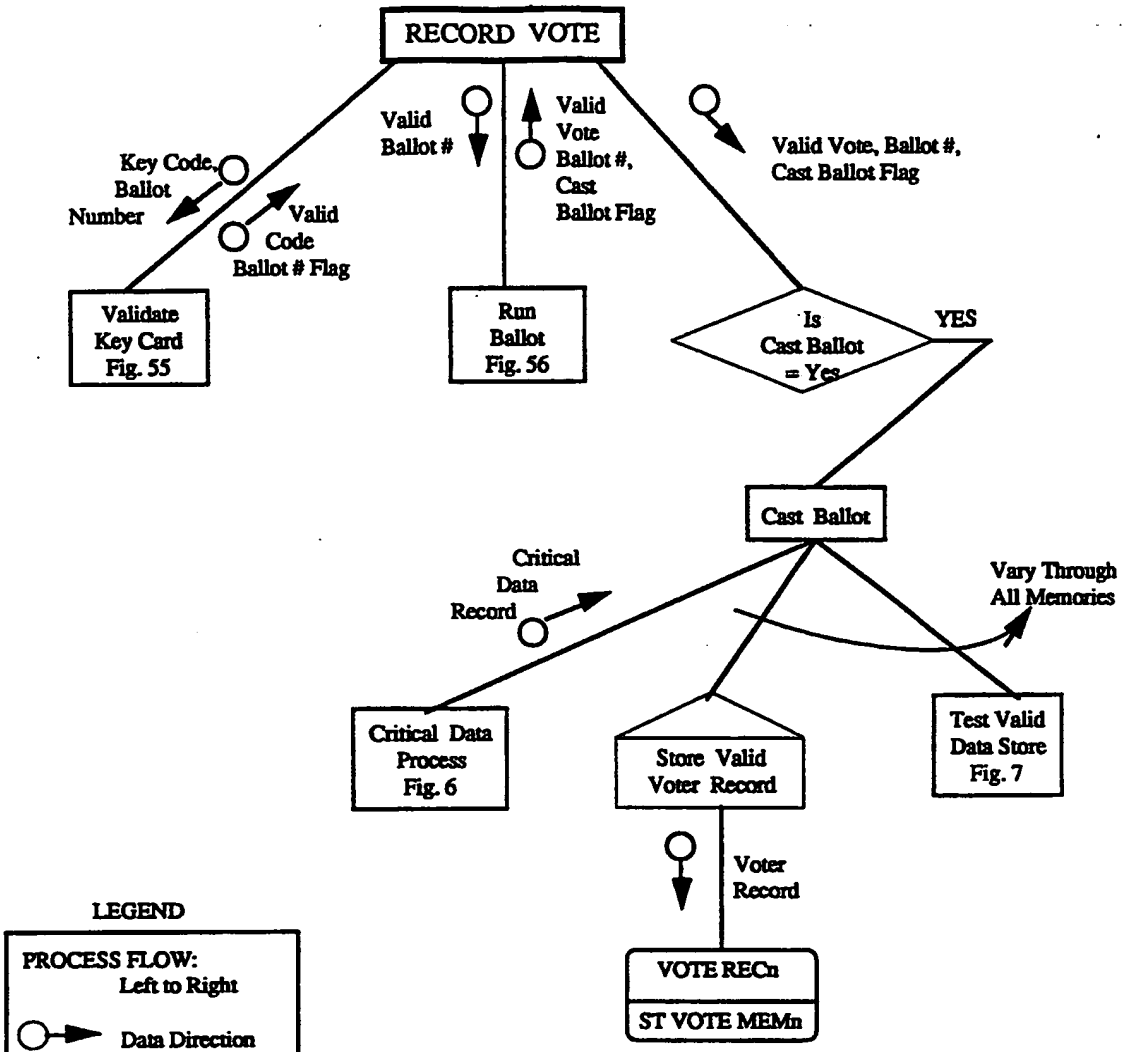
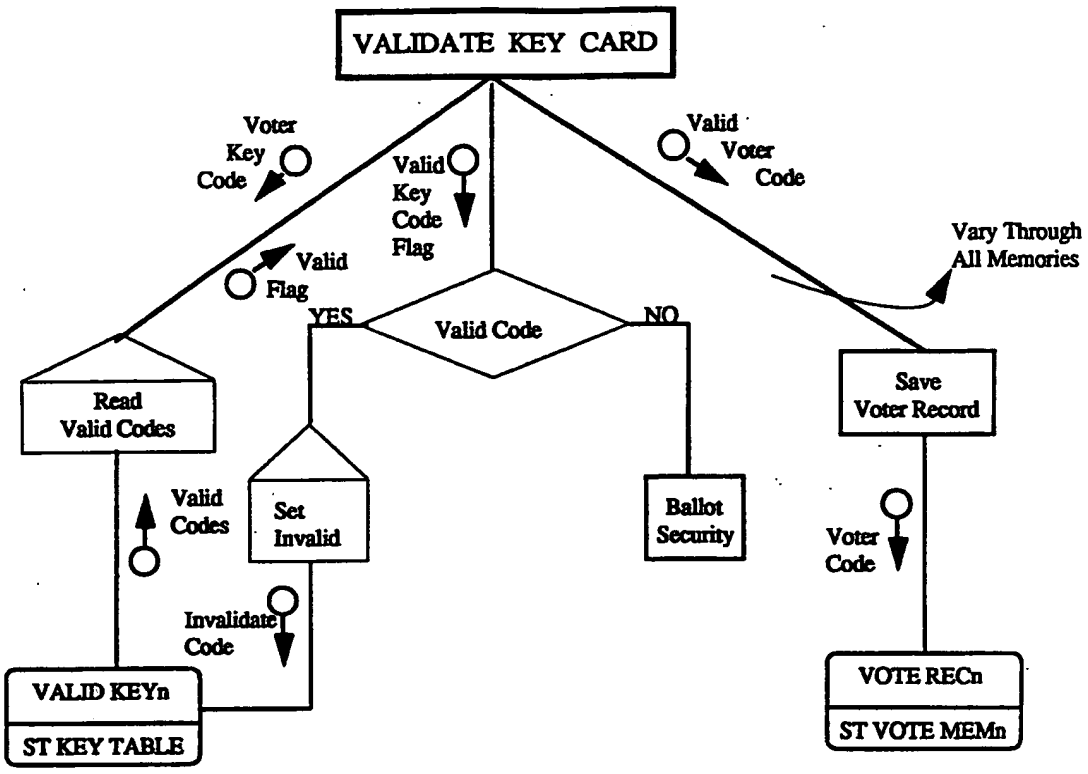


FIGURE 54 • Record Vote



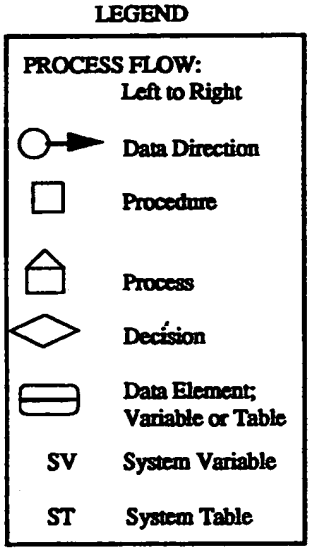
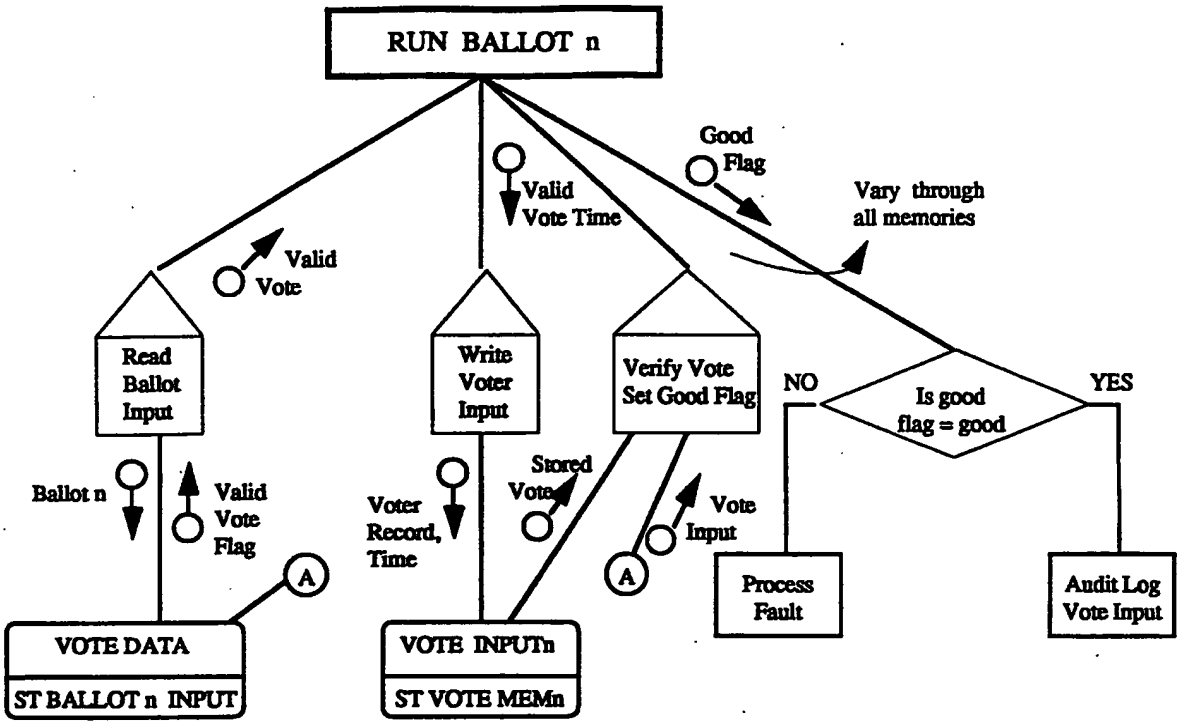


FIGURE 55 • Validate Key Card



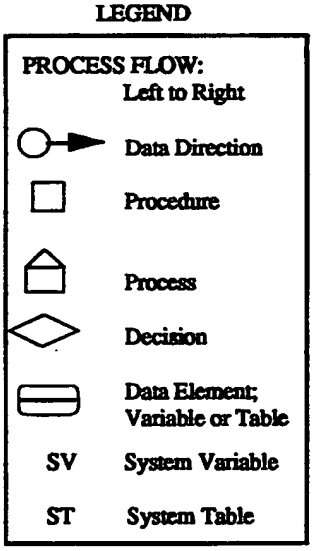
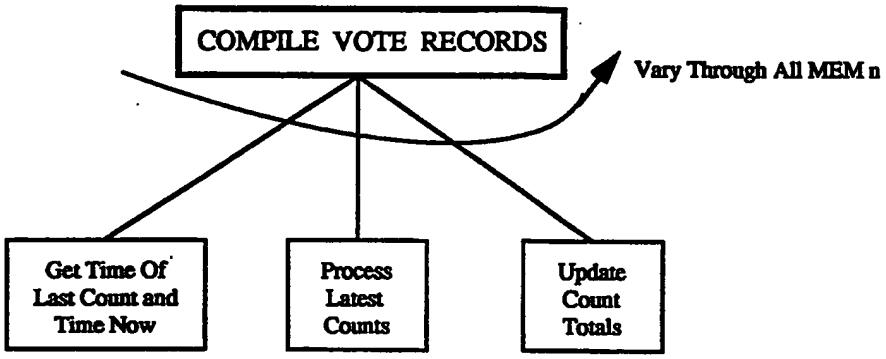


FIGURE 56 • Run Ballot n



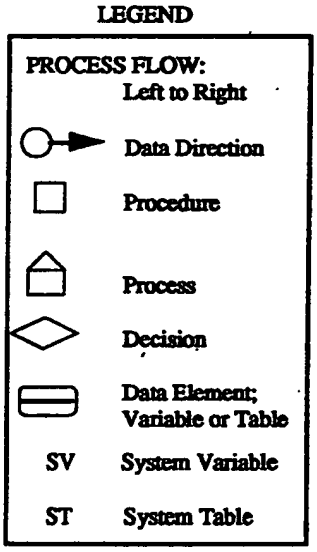
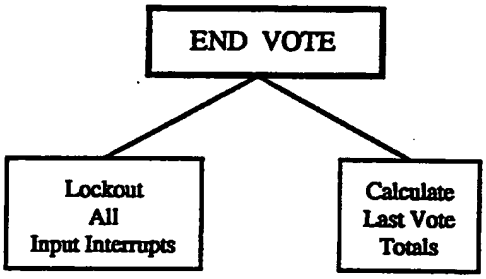


FIGURE 57 • Compile Vote Records



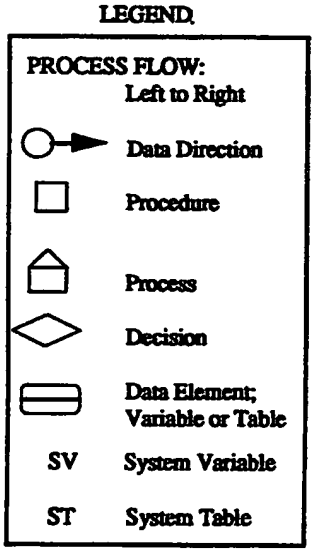
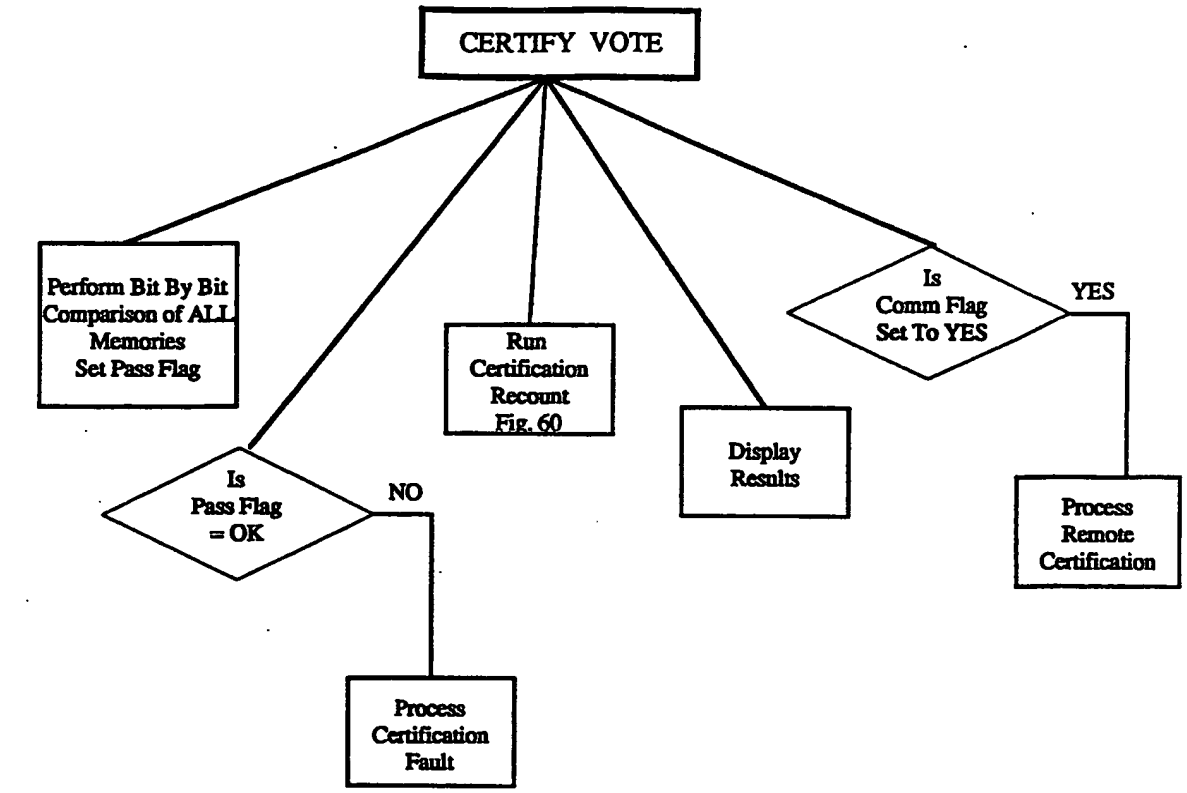


FIGURE 58 • End Vote



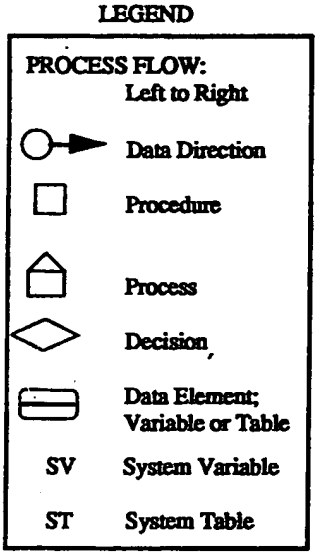
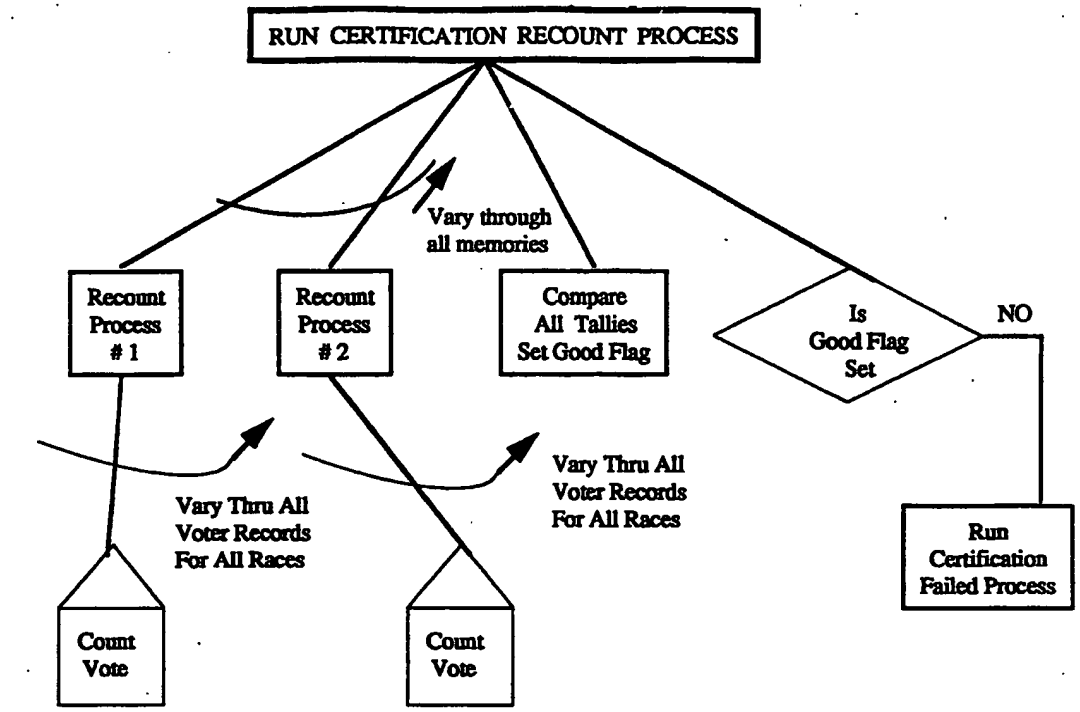


FIGURE 59 • Certify Vote



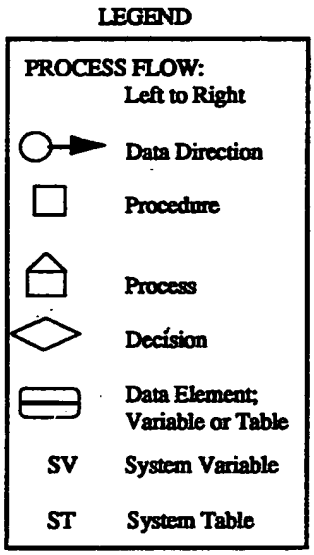
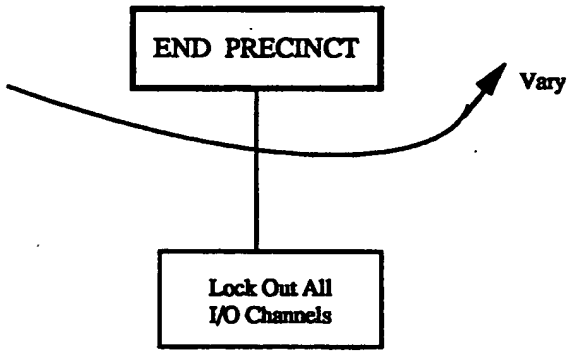


FIGURE 60 • Run Certification Processing



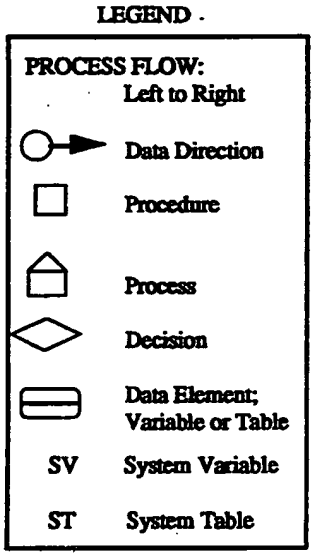
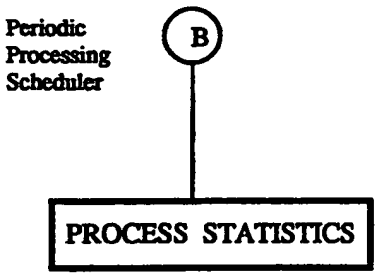


FIGURE 61 • End Precinct



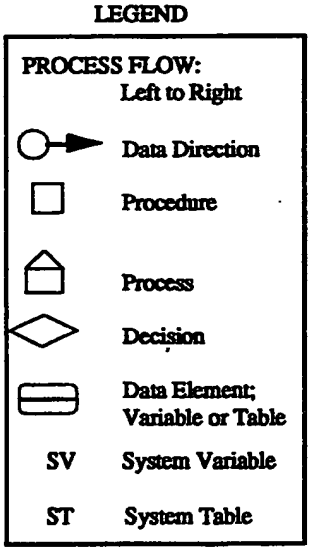
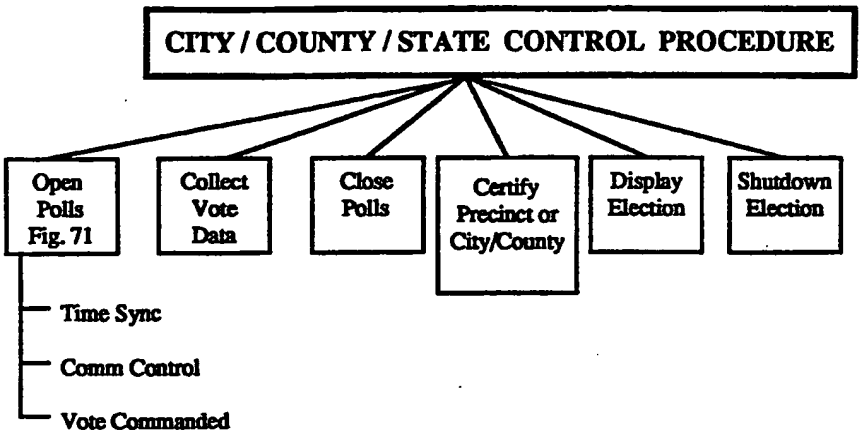
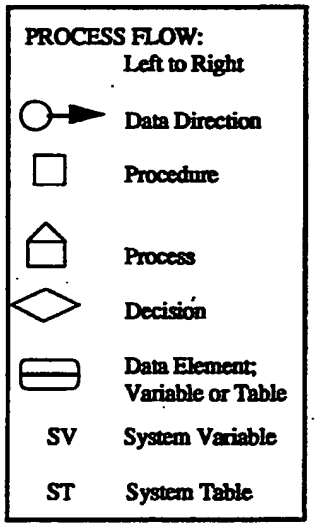


FIGURE 62 • Statistics Processing





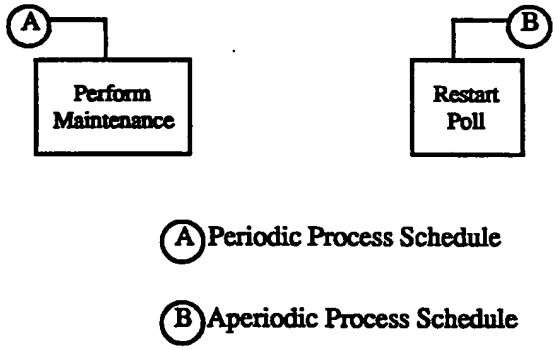


FIGURE 63 • City/County/State Control Processing Functions

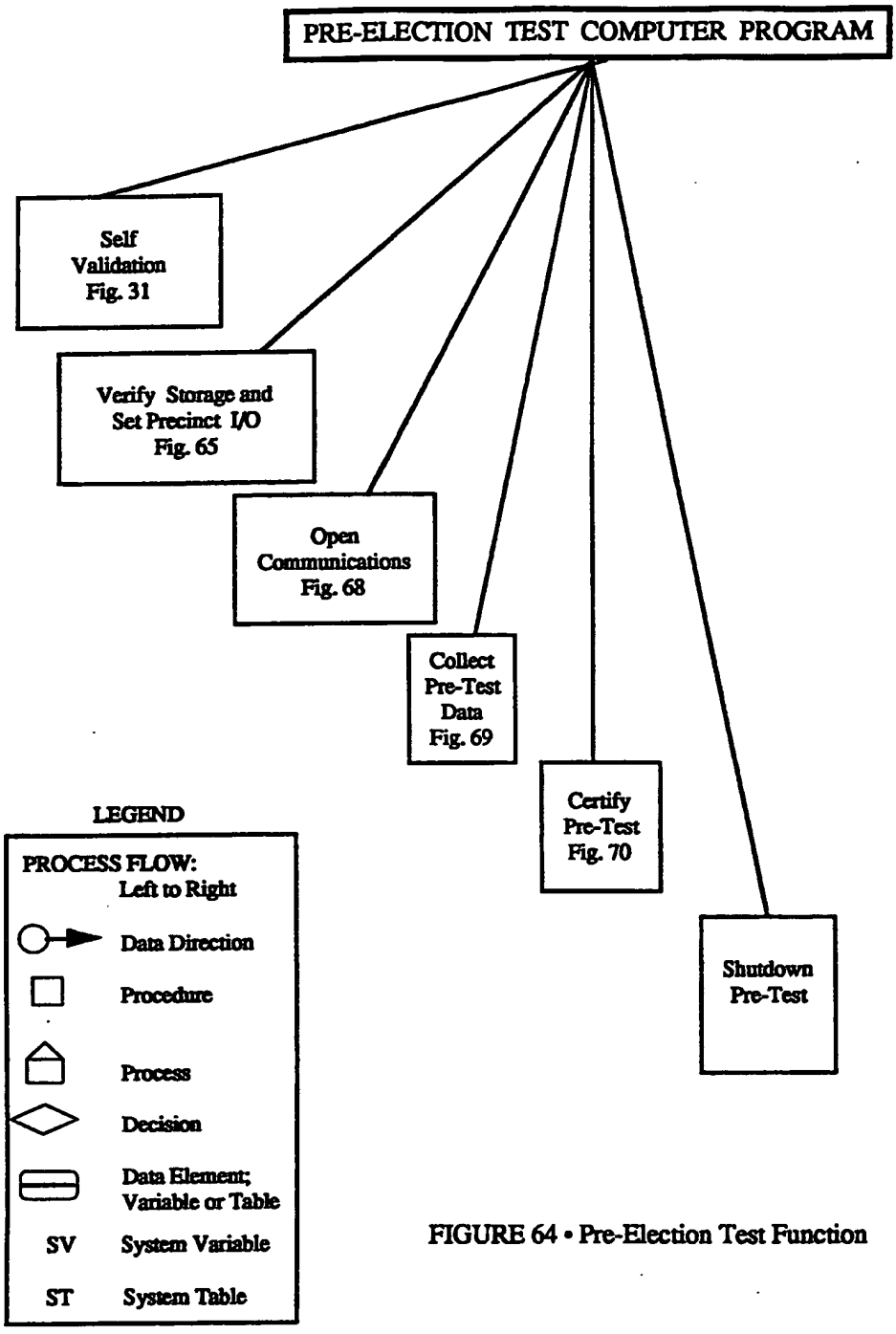
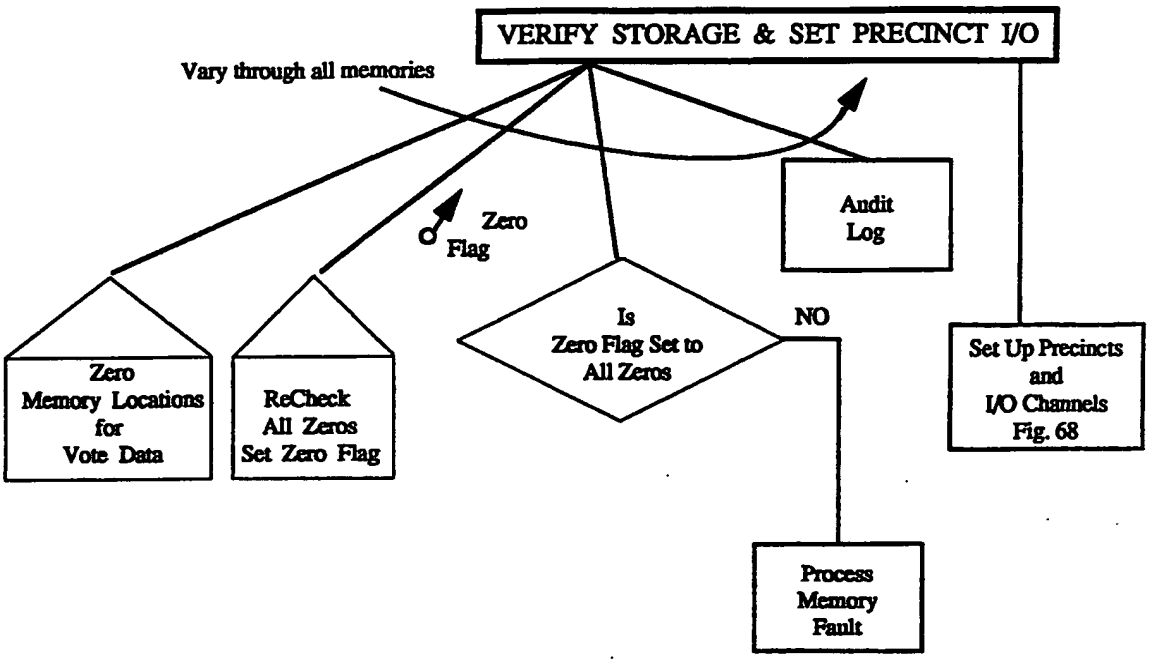


FIGURE 64 • Pre-Election Test Function



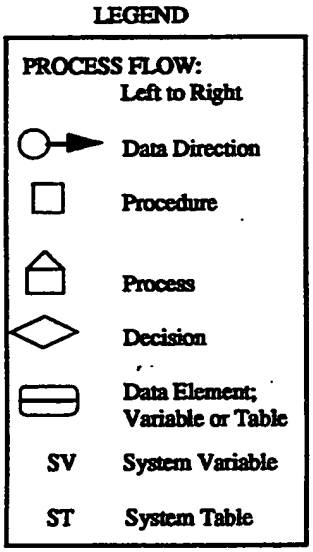
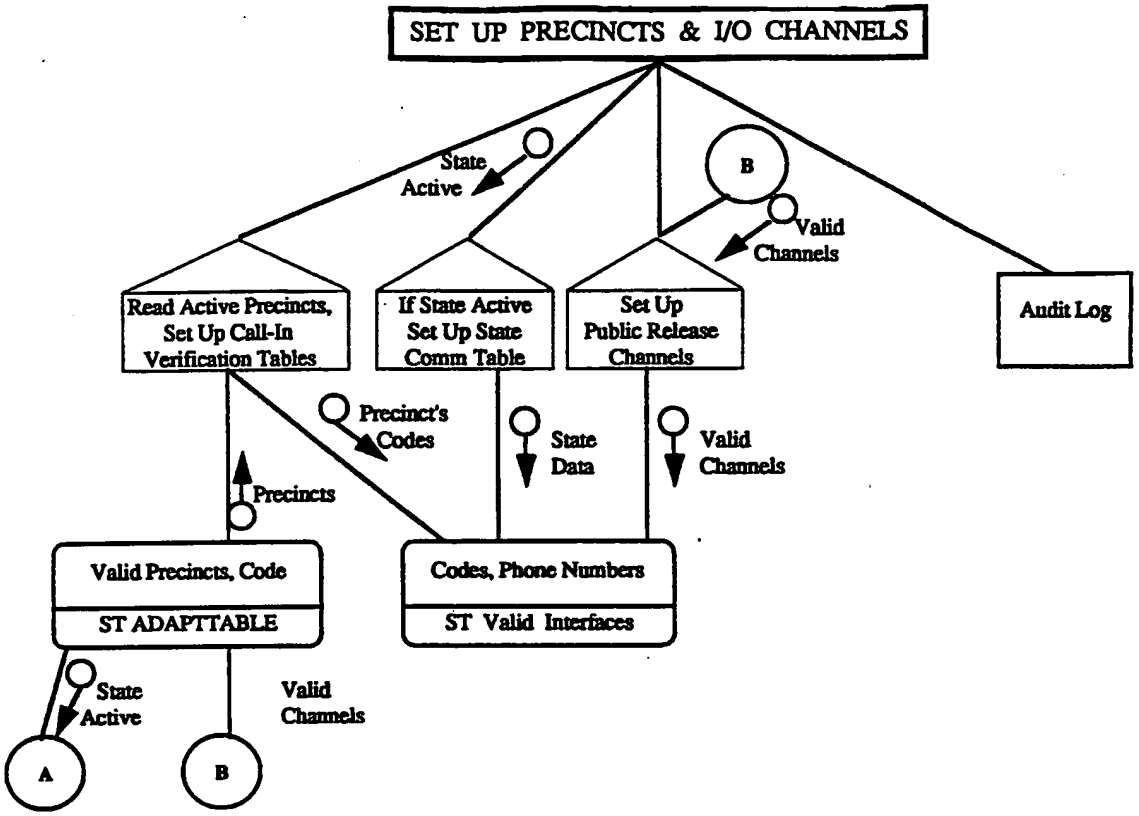


FIGURE 65 • Verify Storage & Set Precinct I/O



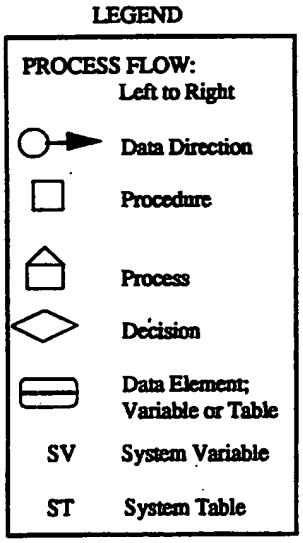
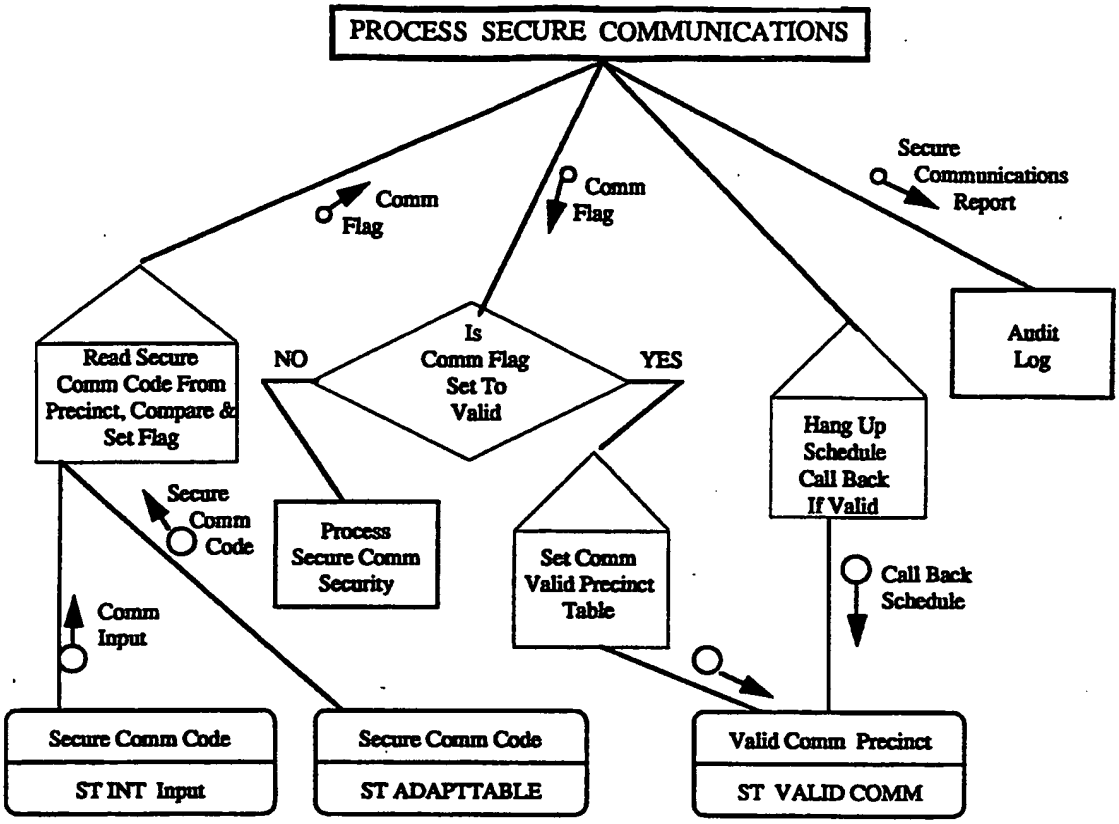


FIGURE 66 • Set Up Precincts & I/O Channels



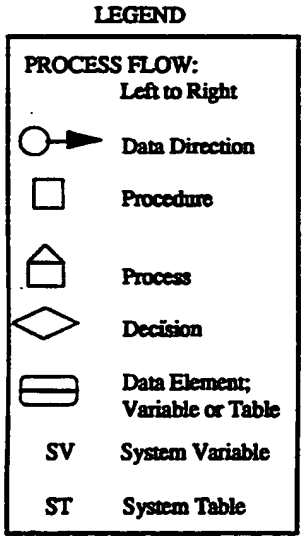
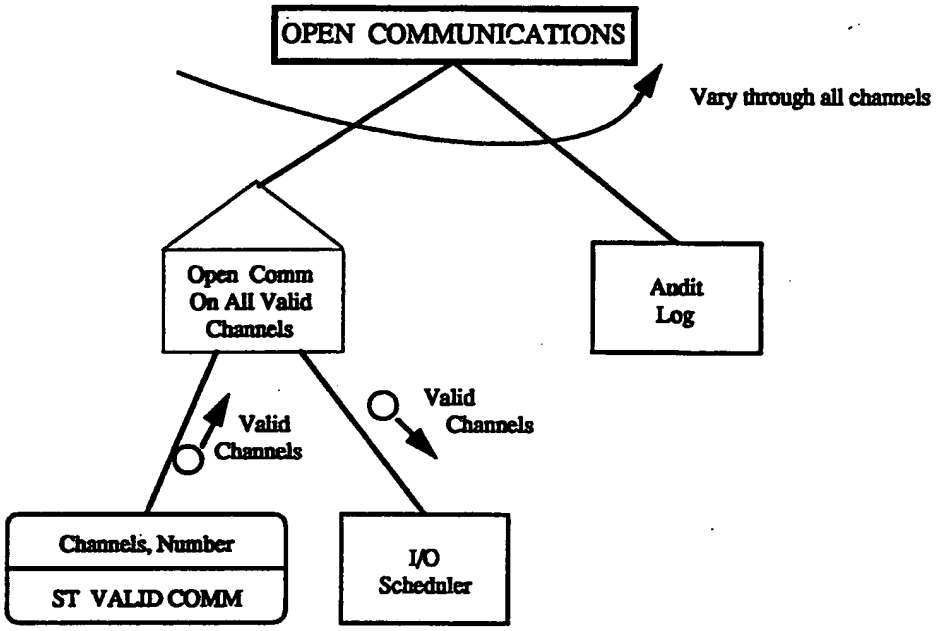


FIGURE 67 • Process Secure Communications



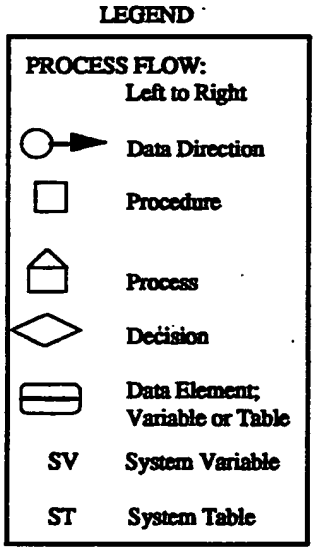


FIGURE 68 • Open Communications

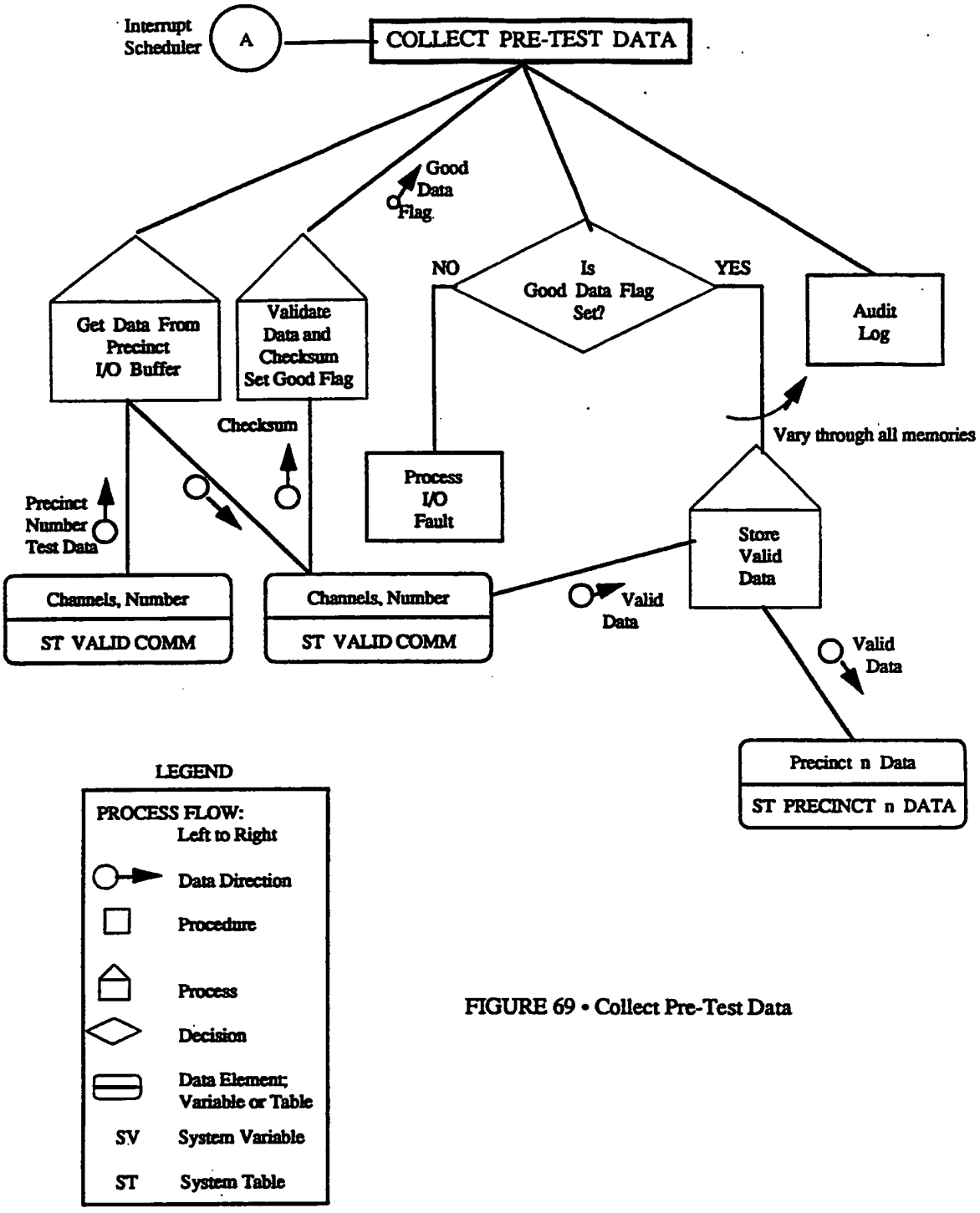
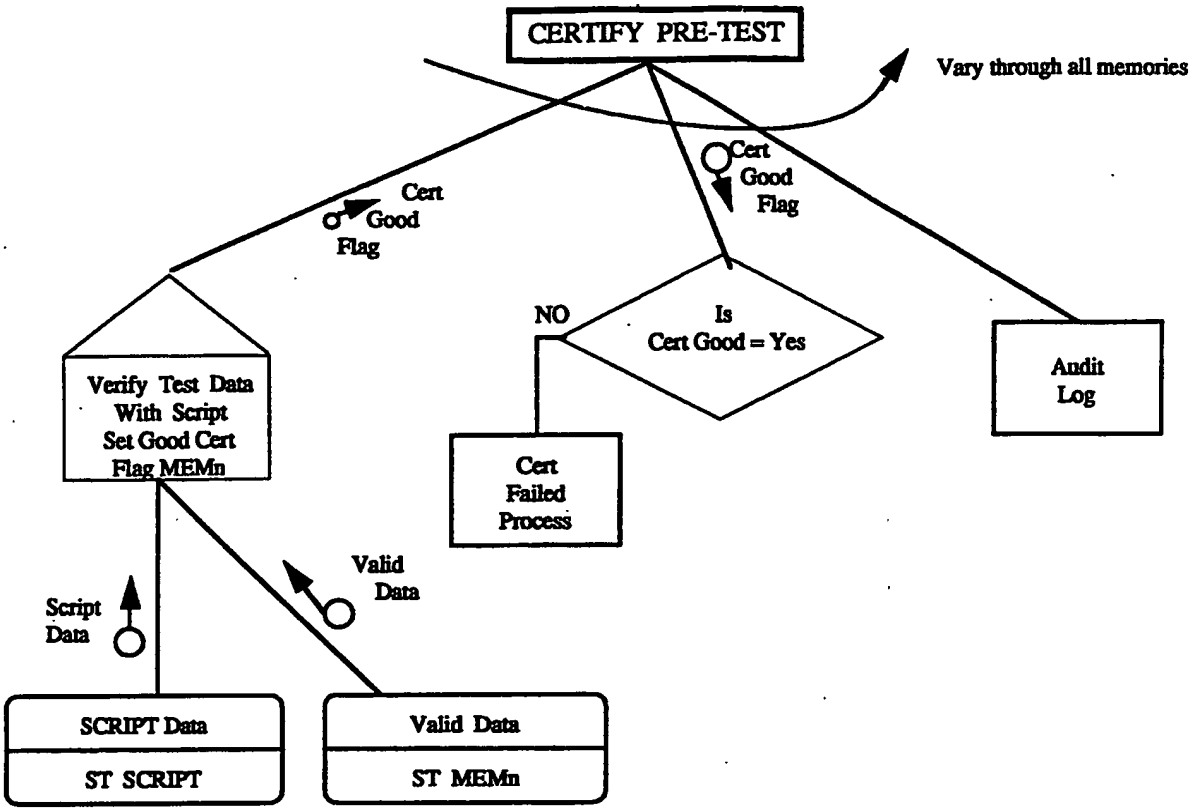


FIGURE 69 • Collect Pre-Test Data



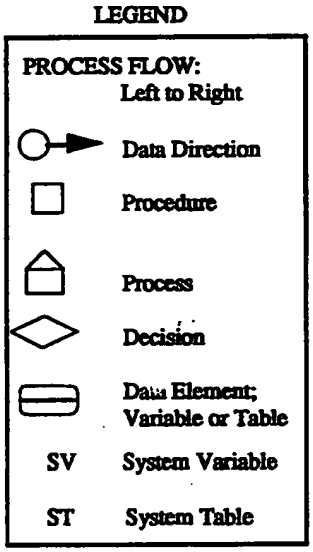


FIGURE 70 • Certify Pre-Test

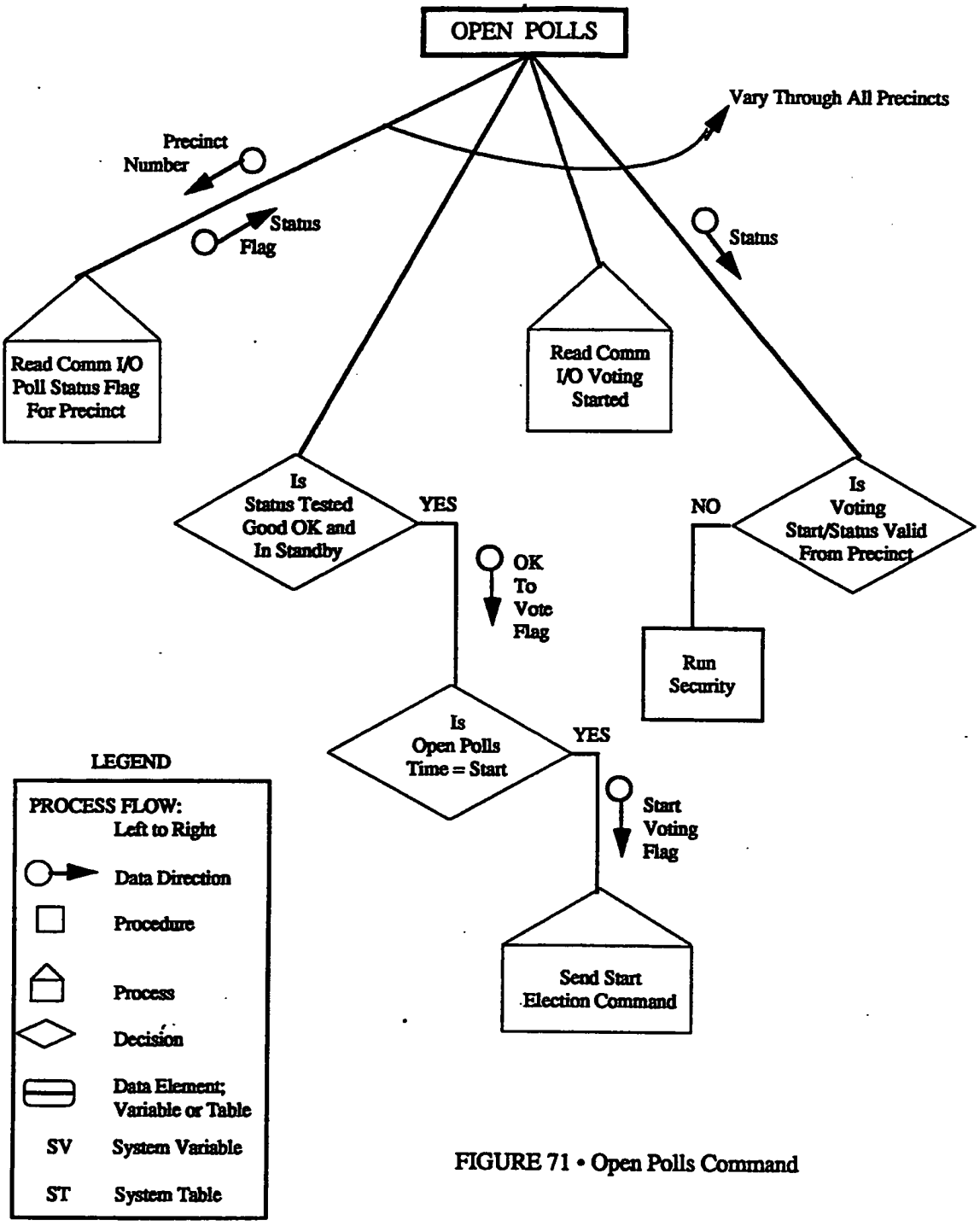


FIGURE 71 • Open Polls Command

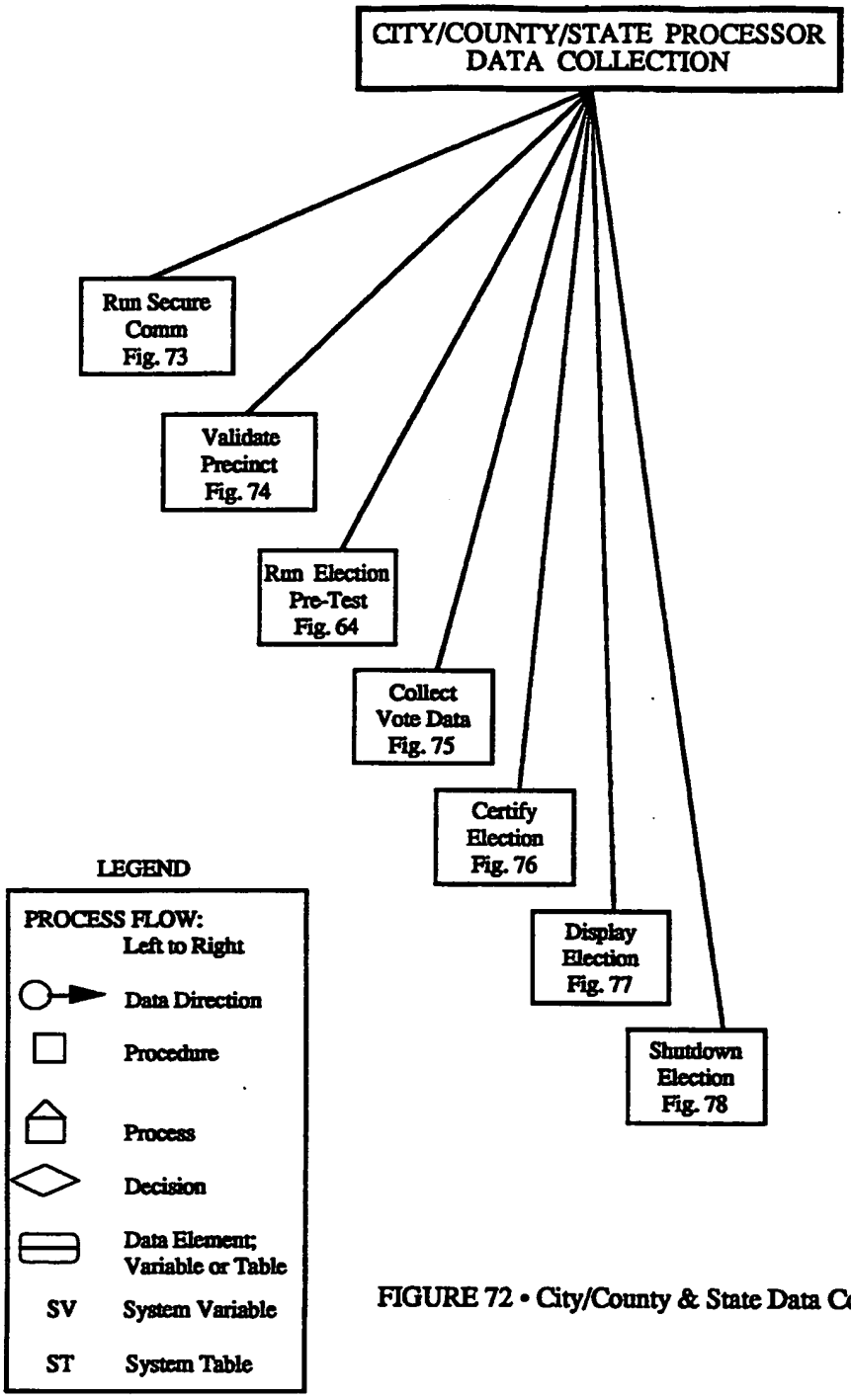


FIGURE 72 • City/County & State Data Collection Processing

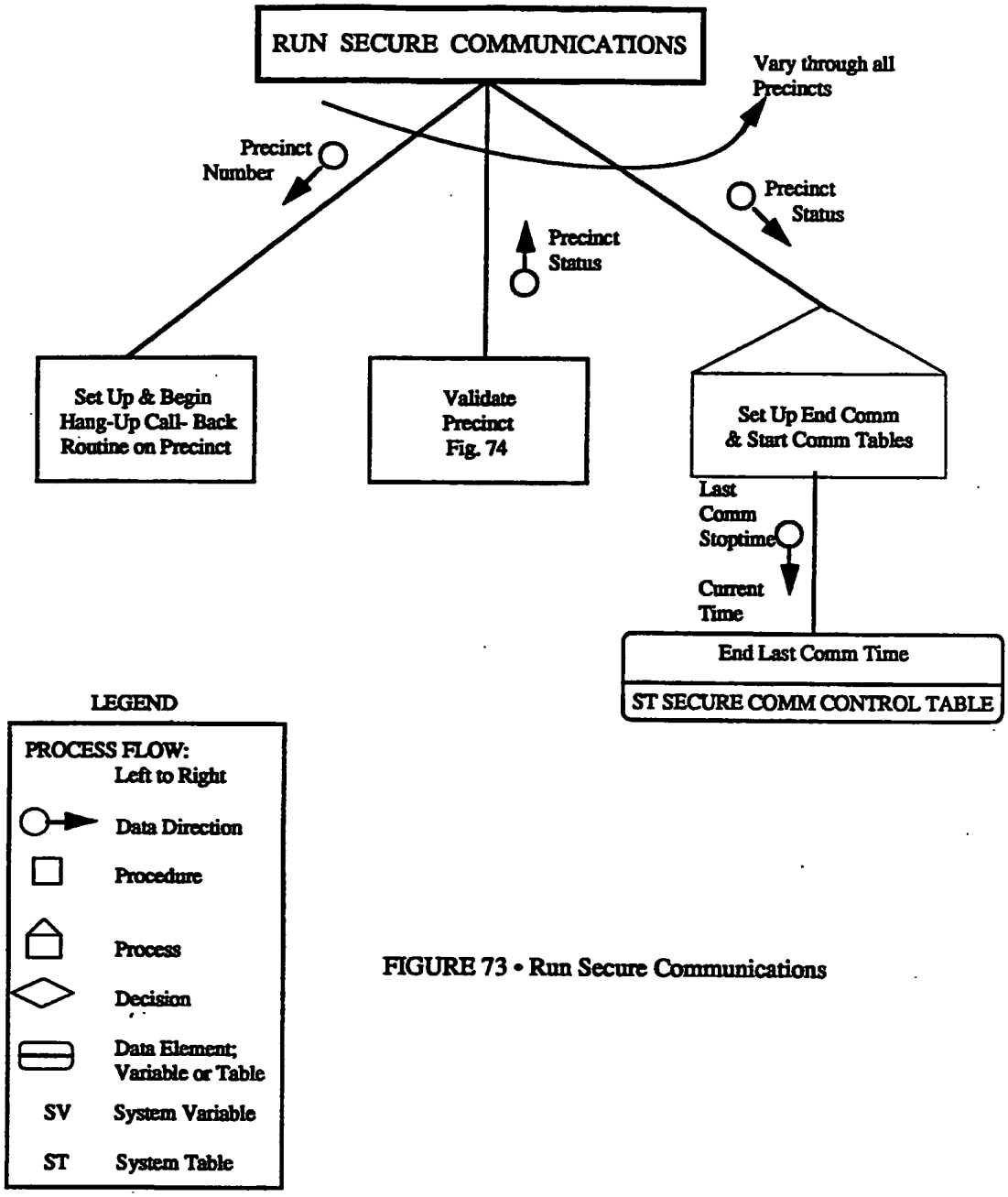


FIGURE 73 • Run Secure Communications

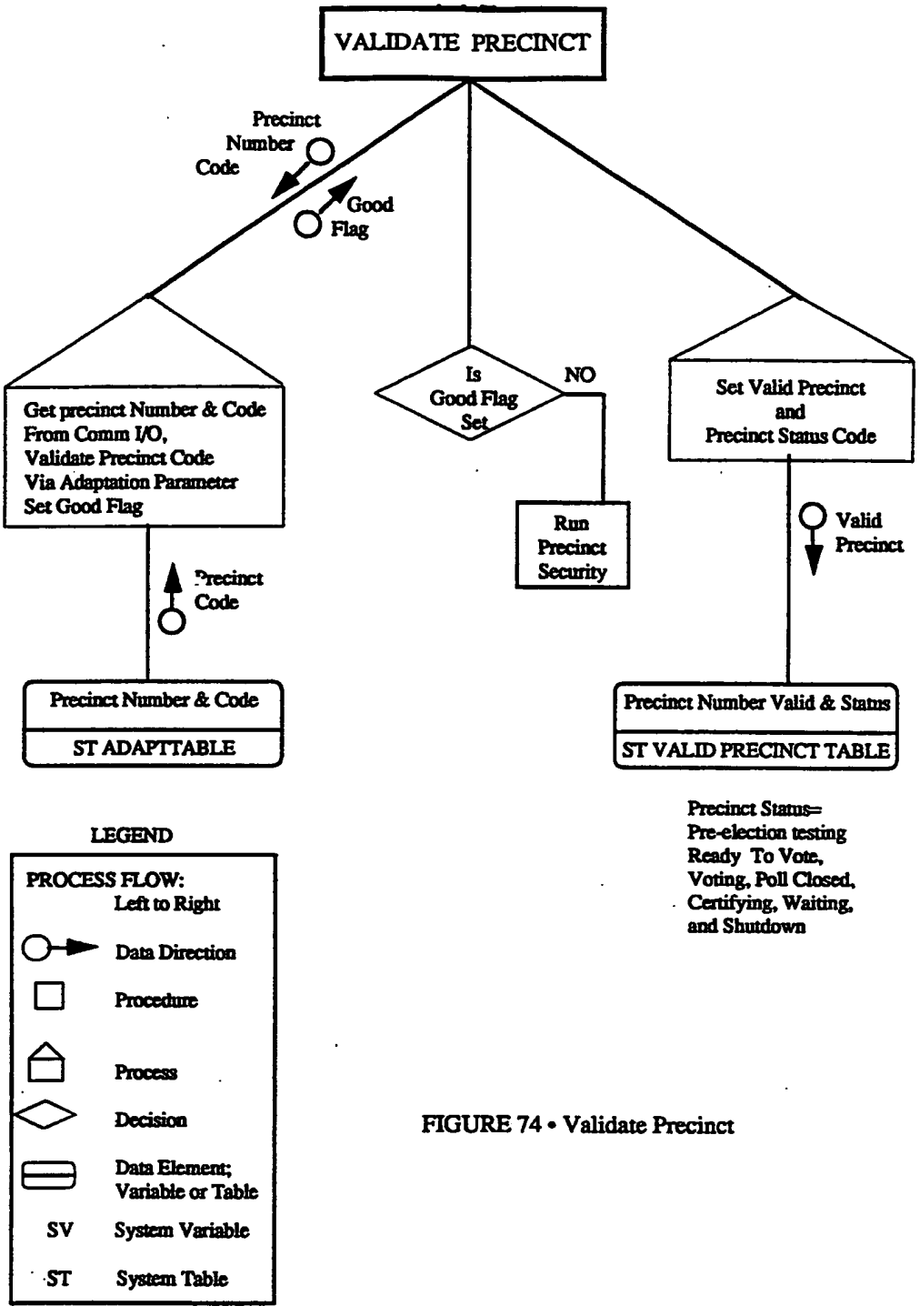


FIGURE 74 • Validate Precinct

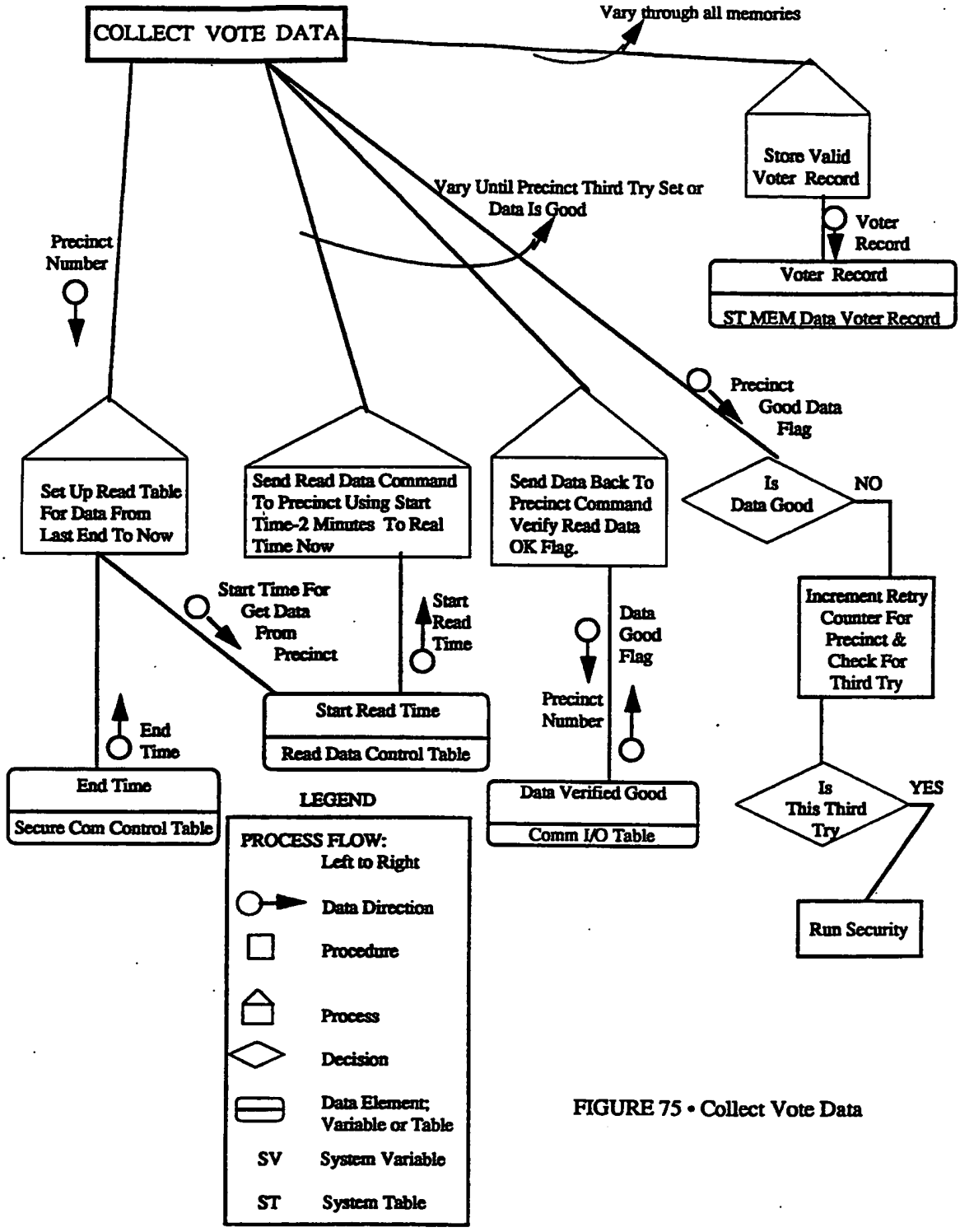


FIGURE 75 • Collect Vote Data

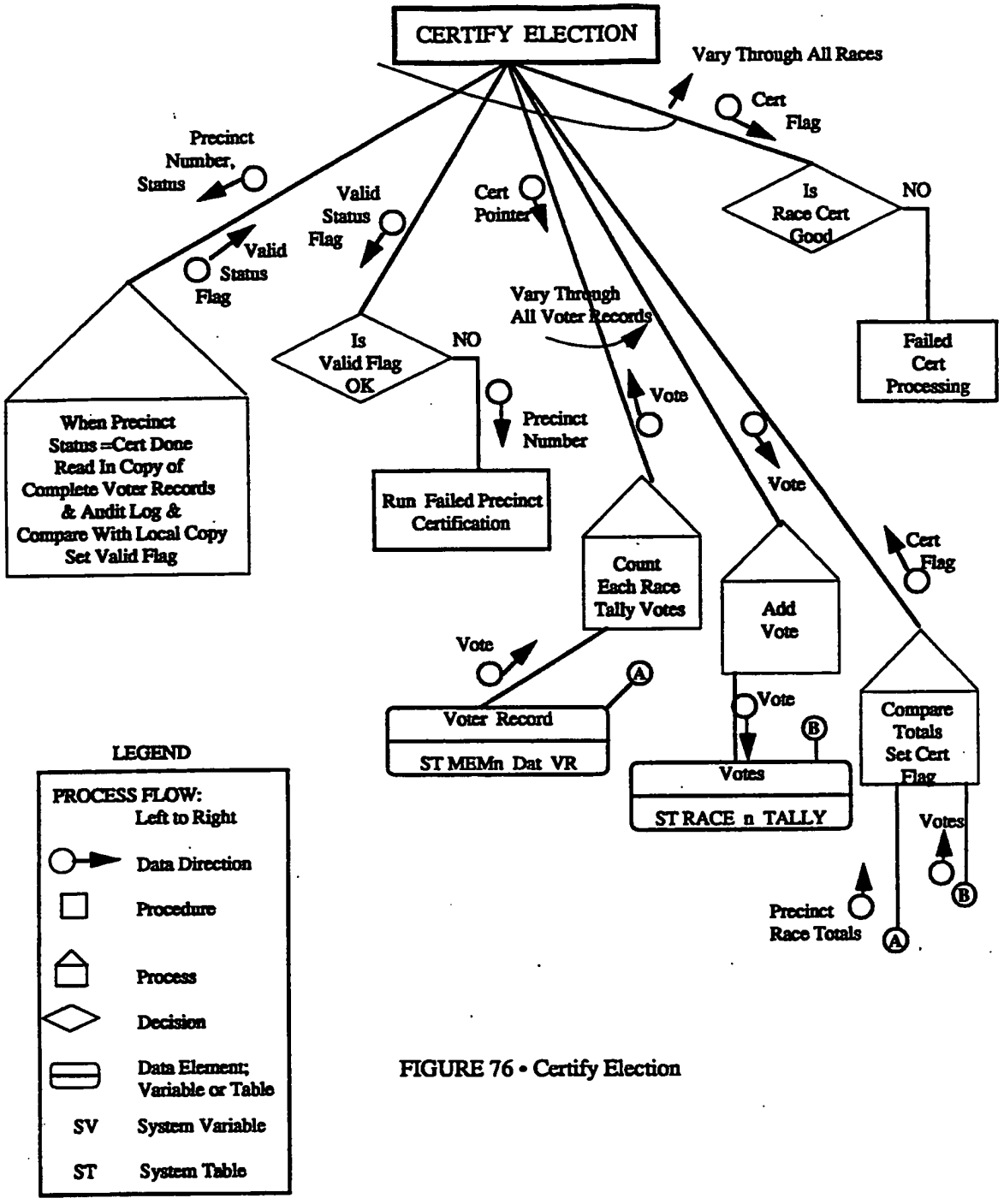
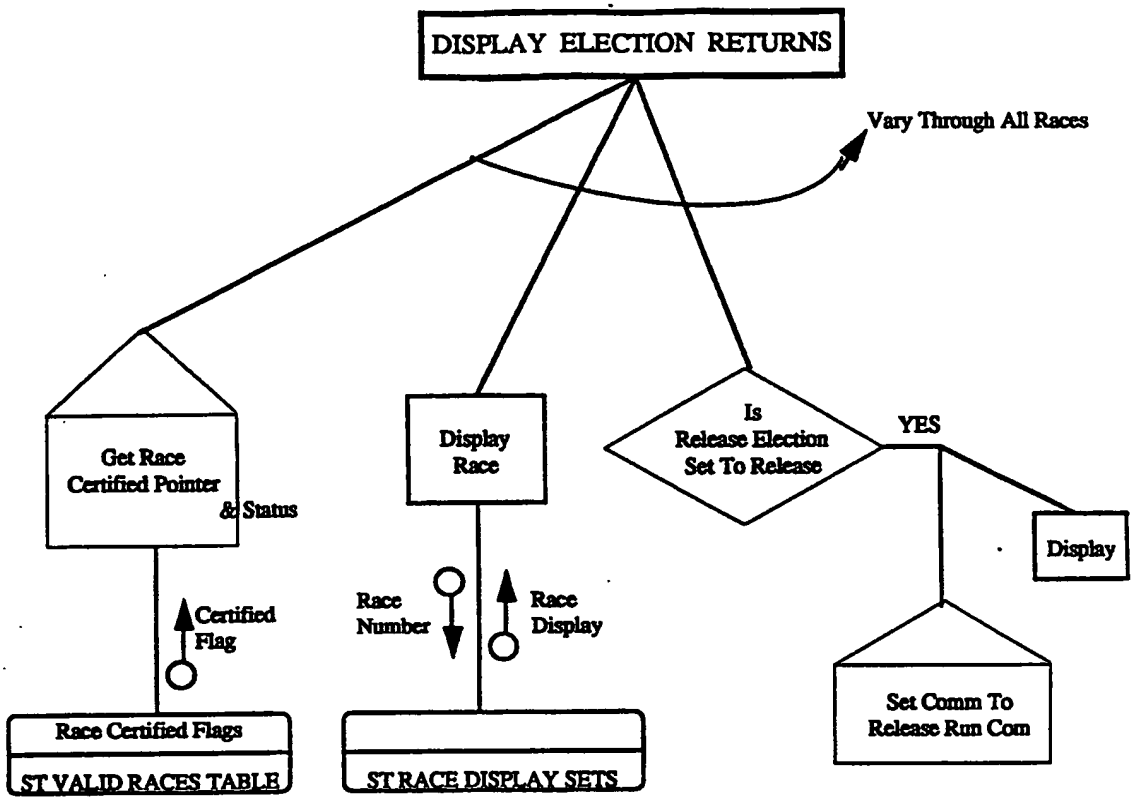


FIGURE 76 • Certify Election



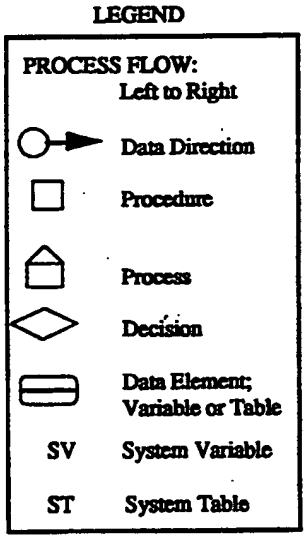
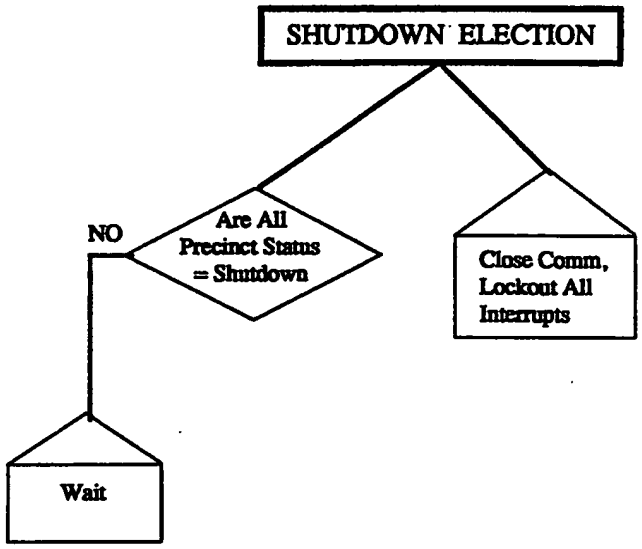


FIGURE 77 • Display Election Returns



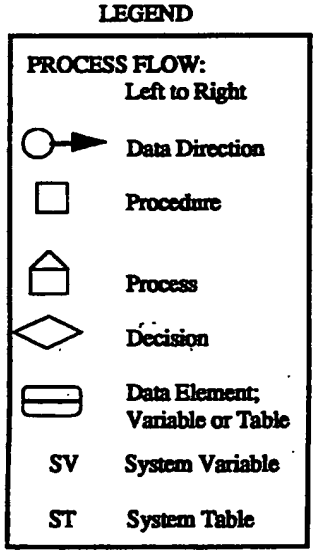


FIGURE 78 • Shutdown Election

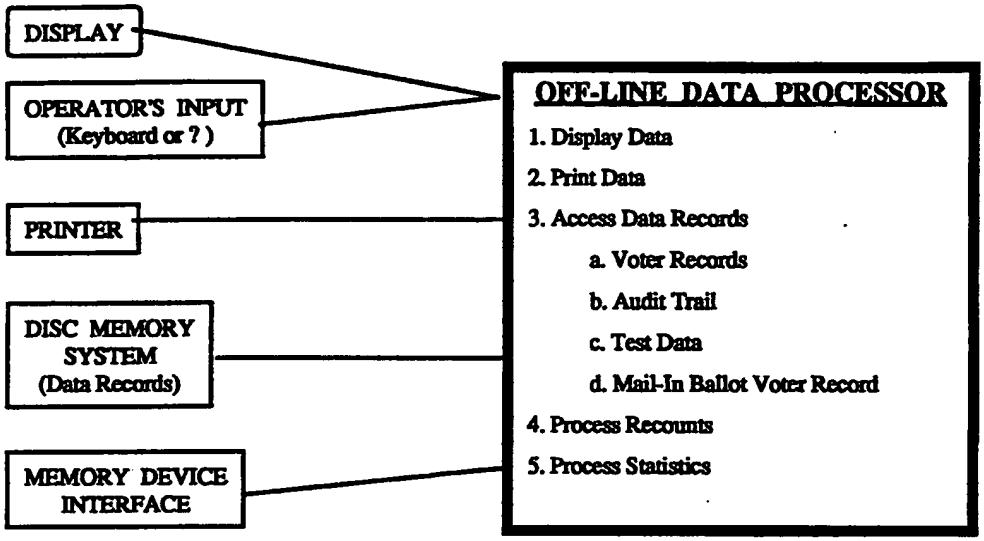


FIGURE 79 • City/County Off-Line Data Processing-
Functional Block Diagram

INTERNATIONAL SEARCH REPORT

national Application No
PCT/US 95/08267

A. CLASSIFICATION OF SUBJECT MATTER

G 07 C 13/00

According to International Patent Classification (IPC) or to both national classification and IPC 6

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G 07 C,G 06 F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, A, 92/03 805 (TECNOMEN OY) 05 March 1992 (05.03.92), fig. 1,2; abstract; page 13, lines 22-24.	15,19
A		1,9-11,16,17,20
A	US, A, 5 218 528 (WISE) 08 June 1993 (08.06.93), fig. 1; abstract; column 3, lines 50-55 (cited in the application).	1,9,15,20
A	EP, A, 0 577 921 (THE CENTER FOR POLITICAL PUBLIC RELATIONS) 12 January	1,9,15,20

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 November 1995	11. 12. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	DRÖSCHER e.h.

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	1994 (12.01.94), fig. 2; abstract; column 3, lines 41,42. --	
A	US, A, 5 189 288 (ANNO) 23 February 1993 (23.02.93), fig. 3; abstract; column 4, lines 27-46 (cited in the application). --	1,9, 15,20
A	US, A, 4 641 240 (BORAM) 03 February 1987 (03.02.87), abstract (cited in the application). --	1,9, 15,20
A	US, A, 4 641 241 (BORAM) 03 February 1987 (03.02.87), abstract (cited in the application). ----	1,9, 15,20

ANHANG

zum internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX

to the International Search Report to the International Patent Application No.

ANNEXE

au rapport de recherche international relatif à la demande de brevet international n°

PCT/US 95/08267 SAE 114694

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présente annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsibilité de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A1 9203805	05-03-92	FI A0 904216 FI A 904216 FI B 86486 FI C 86486	27-08-90 28-02-92 15-05-92 25-08-92
US A 5218528	08-06-93	keine - none - rien	
EP A2 577921	12-01-94	EP A3 577921 JP A2 6028382 US A 5377099	31-08-94 04-02-94 27-12-94
US A 5189288	23-02-93	keine - none - rien	
US A 4641240	03-02-87	keine - none - rien	
US A 4641241	03-02-87	keine - none - rien	